

## **WO02100037**

Publication Title:

**APPARATUS AND METHOD OF FLEXIBLE AND COMMON IPMP SYSTEM  
FOR PROVIDING AND PROTECTING CONTENT**

Abstract:

Abstract of WO02100037

An apparatus of a flexible and common IPMP (intellectual property management and protection) system gives acquiring and mutual operability to the system by fetching a complete IPMP tool list held by a content stream or downloaded from the URL position. The apparatus provides an IPMP tool manager of a conforming IPMP terminal functioning as a pre-processing module, syntactically analyzes the IPMP tool list, and acquires an IPMP tool according to the IPMP tool ID, a position identifier related to it, and the IPMP tool format ID. By pre-compiling the IPMP tool into a binary format, the IPMP tool can be transferred or downloaded to the IPMP terminal, and a different binary format is prepared by a content provider for an object on a different platform of the IPMP terminal.

Data supplied from the esp@cenet database - Worldwide

-----  
Courtesy of <http://v3.espacenet.com>





(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT,

2 文字コード及び他の略語については、定期発行される各 *PCT* ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

柔軟及び共通 I PMP システム (知的所有権管理及び保護) の装置は、コンテンツストリームに保持された、又は URL 位置からダウンロードされた完全な I PMP ツールリストを取り入れることにより柔軟性及び相互運用性を与える。前処理モジュールとして機能する準拠 I PMP 端末の I PMP ツールマネージャを提供して、I PMP ツールリストを構文解析し、I PMP ツール ID、それに関連する位置識別子及び I PMP ツールフォーマット ID に基づいて I PMP ツールを取得する。I PMP ツールを、バイナリフォーマットにプリコンパイルして I PMP 端末に伝送又はダウンロードすることができ、I PMP 端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。

## 明 細 書

## コンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置及び方法

## 5 技術分野

本発明は、コンテンツの提供及び保護に関し、特に保護コンテンツを異なる I PMP システムにより消費する、及び同一コンテンツを異なる I PMP システムにより保護するような用途に関する。

## 10 背景技術

コンテンツ提供は、マルチメディアデータとして益々需要が増大しており、コンテンツは、どこへでもいつでも到達可能である。ユーザは、便利さ及び柔軟性に満足しており、娯楽を容易かつ効率的に楽しむことができる。

一方、コンテンツの所有者は、顧客のニーズを満たすように努力しているが、同時に、それらのプロパティの不正使用にも苦慮している。2つの側面の間のバランスである。

前記コンテンツを保護する保護技法は、データ暗号化、透かし、暗号手法など多数ある。前記保護技法は、多くのコンテンツ提供アプリケーションで実施されている。異なるシステムが異種の機構及び保護技法を使用して保護付きのコンテンツを提供するように見える。その場合におけるすべての端末又はコンテンツ消費装置は、同一のコンテンツプロバイダにより提供されるコンテンツを実行して消費することができるだけである。前記保護技法では、それらの端末又は装置を交換して異なるコンテンツを再生することはできない。

MPEG 標準化グループにおいて、人々は、準拠端末を含む I PMP システムを標準化する方へ努力している。すべての端末は、たとえどのような種類の I PMP ツールを使用しても、次のような同一の I PMP 標準により暗号化されて保護される保護コンテンツを再生することができる。

そのような端末は音声及び映像デコーダのようなコンテンツデコーダから成り、更に、前記端末は、前記コンテンツを復号して再生できる前に前記保護コンテン

ツから保護を解除する必要がある。従って、I PMP ツールリストを含む保護情報は、保護を解除する方法を理解するのに必要とされ、前記端末がコンテンツを利用できるのに必要とされる。

一方、I PMP ツールは予めある特定のツールに固定されない。これは、ベンダがそれらのI PMP システムで好みのツールを選択する柔軟性をより高めることである。このような場合、より高い柔軟性とセキュリティの両方を同時に提供するのにある標準の方法及びインタフェースを定義する必要がある。

そのような端末に関する先行技術が基本的に図1に示してあり、図1は、リアルタイムでユーザ認証、I PMP ツール検索及びコンテンツ復号までの作業の流れを示す。

異なるベンダは、同一のコンテンツデコーダ、例えばMPEG-2又はMPEG-4を使用するけれども、前記先行技術におけるユーザ認証及びI PMP ツール検索は、異なるベンダに関して全く違って実施されている。このような場合に異なるコンテンツプロバイダにより提供される異なるコンテンツを実行するのに同一の端末を製造することは非常に困難である。換言すれば、同一の保護コンテンツを異なるI PMP システムで再生することができない。

## 発明の開示

(発明が解決しようとする技術的課題)

解決すべき課題は、同一のI PMP システム構造を定義して異なるI PMP システムが同一の保護コンテンツを消費可能にすること、及びI PMP システム実施者に対して標準の方法を提供して安全な方法でエンコーダ、チャネル提供から端末までの全システムを構築することである。

(その解決方法)

本発明によれば、柔軟及び共通I PMP システム (知的所有権管理及び保護) の装置は、コンテンツストリームに保持された、又はURL位置からダウンロードされた完全なI PMP ツールリストを取り入れることにより柔軟性及び相互運用性を与える。

前処理モジュールとして機能する準拠 I PMP 端末の I PMP ツールマネージャによって、I PMP ツールリストを構文解析し、I PMP ツール ID、それに関連する位置識別子及び I PMP ツールフォーマット ID に基づいて I PMP ツールを取得する。

- 5        I PMP ツールを、バイナリフォーマットにプリコンパイルして I PMP 端末に伝送又はダウンロードすることができるように、I PMP 端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。

- 10        3 種類の主要かつ一般的なインタフェースは、非常に有用かつ典型的な用途要件に従って、データ暗号解読、透かし埋め込み、及び透かし及びデータ暗号解読の仕方用に指定される。

本発明の一実施例では最小 2 層構造を提案して、ユーザ認証出力メッセージを指定し、異なる I PMP システムに関してより高いセキュリティ及び端末互換性を与える。

- 15        端末複雑性及び I PMP ツール多様性は、I PMP ツールを取得して使用する際に異なるプロファイルを指定することにより処理される。

まず第 1 に、I PMP ツールリストを、コンテンツストリーム内に位置するある特定の packets として定義し、下記の内容を示す。

- ・コンテンツを保護するのに使用される I PMP ツールのリスト
- 20    ・ダウンロードされた I PMP ツールのフォーマット ID
- ・ I PMP ツールの位置タイプ
- ・ I PMP ツールを取得可能な位置

I PMP ツールリストフラグは、上記 packets の前にヘッダとして位置している。

- 25        I PMP ツールマネージャは、コンテンツデコーダの前に位置するあるモジュールとして設計され、コンテンツストリームに保持された、又はどこかに格納された I PMP ツールリストを構文解析して、コンテンツストリームから保護を取り外す為の I PMP ツールを取得する。

汎用のインタフェースが、ダウンロードされた I PMP ツールを I PMP 端末

で利用できる様に I PMP 端末用指定される。このインターフェースはある種のツールに基づいた殆どの異なるアルゴリズムを扱えるように定義される。

2 層のセキュリティ構造を取り入れて、より高いセキュリティを与えると同時に、端末互換性のために任意の異なるユーザ認証方法に関する出力要件を決定する。

I PMP ツール ID は予め定めたテーブルで定義され、前記テーブルを事前符号化又は端末にダウンロードしておいても良い。コンテンツプロバイダ側と端末側の両方は、同一のテーブルを参照して同一の I PMP ツールに同一の I PMP ツール ID を使用する必要がある。

端末は、標準の I PMP ツールと考えられている I PMP ツールを事前に実装していても良いし、前記端末がダウンロード機能を有する場合、コンテンツストリームに保持された I PMP ツールリストに基づいて独自の I PMP ツールをダウンロードしても良い。

暗号化キーは、前記 2 層セキュリティ構造に基づいて更に暗号化して I PMP 情報に挿入され、コンテンツストリームと共に端末へ伝送される。

コンテンツプロバイダ側では、メディアコンテンツは、MPEG-2 又は MPEG-4 のような符号化技術を用いて符号化され、DES 又は AES のような I PMP ツールを用いて暗号化される。前記コンテンツは、符号化前に透かしを埋め込まれても良い。

同時に、コンテンツ ID は、コンテンツ著作権情報、コンテンツ作成情報などに基づいて生成される。また、I PMP ツールリストは、コンテンツを保護する際に使用される I PMP ツールに基づいて生成される。前記 I PMP ツールリストは、I PMP ツール ID、I PMP ツールフォーマット ID、位置タイプ、I PMP ツールの位置及び予約フィールドを含む。位置識別子は、位置タイプ及び位置詳細が特定の I PMP ツール ID に従うので、特定の I PMP ツールと密接に関連がある。

I PMP ツールリストフラグは、その後に続くものが I PMP ツールリストであることを示す。

任意の端末は、そのようなコンテンツを取得又は検索できるが、適切な使用ラ

イセンス及び対応する又は正しい I PMP ツールなしに再生はできない。

端末側では、I PMP ツールリストを I PMP ツールマネージャモジュールに渡し、I PMP ツールを取得する。

5 取得された I PMP ツールは、端末で使用可能なものであり、I PMP 端末に格納されて予め定めたインタフェース用に用意がされる。

コンテンツストリームが、コンテンツデコーダを通過し始めると、I PMP システムは、ユーザ認証モジュールを起動して、ユーザ端末 ID、コンテンツ ID 及びその他の関連情報を与えることによりコンテンツプロバイダ又は提供エージェントにセンス要求を送信する。ライセンスは、ユーザ認証がうまく行われた後、  
10 端末に発行される。

最後に、暗号化されたキーは暗号解読され、暗号化されたコンテンツも暗号解読され、コンテンツは端末で復号及び再生可能となる。

#### 図面の簡単な説明

15 図 1 は、先行技術のコンテンツ提供及び保護の既存 I PMP システムを示す。

図 2 は、準拠 I PMP システムの一般図を示す。

図 3 は、コンテンツストリームに保持された I PMP ツールリストパケットの構成を示す。

20 図 4 は、MPEG-4 の I PMP システムと共に作動する I PMP ツールマネージャの構成を示す。

図 5 は、MPEG-2 のシステムと共に作動する I PMP ツールマネージャの構成を示す。

図 6 は、MPEG-4 の I PMP システム及び I PMP ツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

25 図 7 は、MPEG-2 のシステム及び I PMP ツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

図 8 (a) は、エンコーダを有する部分的暗号化の構成を示す。

図 8 (b) は、エンコーダを有しない部分的暗号化の構成を示す。

図 8 (c) は、部分的暗号解読の構成を示す。



図 9 は、本発明の他の実施例の I PMP システムの構成図を示す。

図 1 0 は、本発明の実施の形態における I PMP システムにおいて、プロバイダからユーザ端末に送られるメッセージの流れ図を示す。

図 1 1 は、メッセージの具体例を示す。

5 図 1 2 は、メッセージ内の I PMP 情報の一例を示す。

図 1 3 は、利用規則管理モジュールの処理フロー図を示す。

発明を実施するための最良の形態

図 1 は、現在の典型的な I PMP（知的所有権管理保護）システムを示す。

10 ユニット 1. 0 のコンテンツ所有者は、ユニット 1. 1、1. 5 及び 1. 9 の異なるコンテンツプロバイダ A、B 及び C を通してコンテンツを提供する。異なる I PMP システムは、3 組の I PMP システムで実施されている。

15 各々のプロトコルが異なる I PMP ツール（例えば暗号化ツール）及び異なるユーザ認証ツールなどを使用しているので、I PMP ツールを取得して検査する方法はそれら自体のプロトコルに基づく。異なるユーザ認証方法は、ユニット 1. 2、1. 6 及び 1. 1 0 に示してあり、I PMP ツールを取得する異なる方法は、ユニット 1. 3、1. 7 及び 1. 1 1 に示してある。

20 従って、ユニット 1. 4、1. 8 及び 1. 1 2 に示すように、コンテンツ復号又はコンテンツ消費端末も互いに異なる。端末 A がコンテンツプロバイダ B により提供される保護コンテンツを再生することはできないということが明らかである。

以下の内容については、本願発明者による先の出願（特願 2 0 0 1 - 0 5 8 2 3 6）において解決された。

25 1) I PMP ツール情報をストリームに保持して、コンテンツプロバイダ及びコンテンツディストリビュータにより何れの I PMP ツールを使用するかを表示すること。

2) 準拠 I PMP 端末で I PMP ツール管理を用いて I PMP 情報を処理すること。

3) 異なる処理能力を有する I PMP 端末に関するプロファイルを定義して、I

PMPシステムを実現すること。

しかし、先の出願では未解決の問題点が2つあり、次のとおりである。

1) 端末OS及びプラットフォームに依存するダウンロードツールフォーマットの問題。

5 2) I PMP端末で使用されるべきI PMPツール用のインタフェースの問題。

本願では、更に、先の出願で提示されたI PMPシステムをより詳細かつより完全な形態で説明し、2つの問題点を詳細に扱って説明する。

図2は、MPEG-nのI PMPシステムを示す。

サーバは、モジュール2. 1で示され、コンテンツプロバイダかコンテンツディストリビュータの何れかとして機能し、又は異なる用途シナリオの場合には両方の機能を果たす。

ネットワーク層は、モジュール2. 3で示され、準拠I PMP端末とサーバとの間の通信及び前記サーバから前記端末へのコンテンツストリームの伝送を行う。

最初は、モジュール2. 4の権利認証が、前記サーバと対話し始めて、権利認証モジュールの出力メッセージのような詳細な使用規則と共にコンテンツアクセス及び消費権利を得る。予め決められたフォーマットのこれらのメッセージは、後で使用されるために前記端末のメモリに格納される。出力メッセージ欄を指定する詳細については、後で説明する。

モジュール2. 4でコンテンツアクセス用権利が許可されると、前記サーバは、前記ネットワーク層を介して要求されたコンテンツストリームを前記端末に送信する。

モジュール2. 2では、他の専用プラットフォーム及びOS用の他のフォーマットに加えてJBC (Javaバイトコード)、DLL (ダイナミックリンクライブラリ) などの異なるフォーマットのバイナリツールに加えて、ツールID、ツール位置ID、ツールフォーマットIDを含むツールリスト情報と共にコンテンツストリームを伝送する。ツールリスト情報を指定する詳細については、後で説明する。

モジュール2. 5に示すI PMPツールマネージャでは、ツールリスト情報を構文解析／解釈すると同時に、ツール位置ID及びツールフォーマットID情報

に従って I P M P ツールを検索する。モジュール 2. 5 からの出力メッセージは、ツールの内容を示す記述子用ツール I D を有する適切な I P M P ツールである。

I P M P ツール自体は、I P M P 基準で予め決められた共通ツールフォーマット I D に基づいた端末プラットフォーム用に選択し検索して適合するバイナリフォーマットである。

ライセンス／キー及び使用規則は、更なる処理のためにモジュール 2. 6 のように前記端末のメモリに格納される。対応するツール I D を有するバイナリ I P M P ツールは、モジュール 2. 7 のように前記端末のメモリに格納される。前記ツールの各々は、一般的な標準化インタフェースに従って構築され、プラットフォームに適合させる為にコンパイラを用いてプリコンパイルされる。例えば、データ暗号化及び暗号解読のツールは、1 つの汎用指定インタフェースに基づいて構築可能である。たとえば、J a v a 仮想マシンで全プラットフォーム／端末用の J a v a バイトコード ( J B C ) にプリコンパイル可能であり、また W i n d o w s によるプラットフォーム／端末用のダイナミックリンクライブラリ ( D L L ) にプリコンパイル可能である。

バイナリ形式のツールは、z i p 形式などの圧縮形式で伝送可能である。前記ツールは、不正変更防止ソフトウェアを用いることにより不正変更可能であり、又は、バイナリコードが破られる又はハッキングされるのを防ぐ署名技法を用いて署名可能である。

モジュール 2. 8 は、I P M P ツールプロバイダ及び端末実施者が予め定めら従うことが必要な I P M P ツール用のインタフェースを示す。

ベース層は、モジュール 2. 9 に示すコンテンツデコーダ及びプレゼンタである。この層は、前記ベース層の他の構成要素に位置して前記構成要素とともにスムーズに動作するバイナリ形式で I P M P ツール用のフックインタフェースを用いて構築される。

汎用インタフェースは、3 種類の I P M P ツール ( 暗号解読用インタフェース、透かし埋め込み用インタフェース、透かし技能と暗号解読用インタフェース ) について後で明記する。権利認証用インタフェースは、用途に大きく左右されるので予め定義することができず、そのため、ここで定義及び固定されるのではなく

パラメトリックツールにより処理される。

詳細な説明をここで4つの部分に分けて、説明する。

#### 1. I PMP ツールリスト及び I PMP ツールマネージャ

##### 1. 1 I PMP ツールリスト及び I PMP ツールマネージャの定義

5 I PMP の概要において、I PMP 情報は、所与の I PMP ツールが所与の保護コンテンツを要求して正しく処理する情報と定義されている。

I PMP ツールは、予め決められた方法で認証、暗号化、透かしなどの I PMP 機能を実行するモジュールであると定義されている。

この発明において、I PMP ツールリストの定義を導入する。

10 I PMP ツールリストは、I PMP ツールマネージャが I PMP ツールを識別して前記 I PMP ツールを検索する必要がある情報を含む。それは、I PMP ツールの一意的識別、I PMP ツールの位置識別子、及び I PMP ツール ID とコンテンツ ID との間の関係定義を含む。

また、I PMP ツールマネージャを次のように定義する。

15 I PMP ツールマネージャは、その唯一の役割が I PMP ツールリストを処理してコンテンツストリーム全体を消費するのに必要な I PMP ツールを検索するエンティティである。

##### 1. 2 I PMP ツールリスト

20 この I PMP ツールリストパケットの詳細構造は、次のような図 3 に最もよく示されている。

前記 I PMP ツールリストパケットは、保護コンテンツを消費するのに必要な全 I PMP ツールの情報を含む。前記コンテンツが 2 種類以上のコンテンツを含む場合、例えば、前記コンテンツの第 1 の部分はコンテンツプロバイダ A からであり、第 2 の部分はコンテンツプロバイダ B から来ている場合、個々の I PMP ツールに関連する情報は、それぞれ関連するコンテンツ ID ごとに分類される。

次に、各コンテンツ ID 用の I PMP ツールリストは、個々の I PMP ツール情報から成れば良く、これらの個々の I PMP ツール情報の順序は重要でない。

各 I PMP ツール情報は、3つの主要な部分、即ち I PMP ツール ID、I PMP ツール位置識別子及び I PMP フォーマット ID から成る。

前記 IPMP ツール ID は、所定の方法でツールを識別し、少なくとも 2 つの部分、ツールタイプ ID 及びツールサブ ID を有する。

ツールタイプ ID は、この特定の IPMP ツールが（ツール機能の点から）何れのカテゴリ、例えば暗号解読、透かし抽出、透かし検出、権利抽出などに属するかを指定する。下記の表は、IPMP ツールの 16 カテゴリを扱うことができる 4 ビットとしてツールタイプ ID の長さを仮に設定する。

更に、ツールサブ ID はある特定の IPMP ツールを識別し、前記サブ ID は、下記の表のように、1 ツールタイプ間の 4096 の異なるツールを識別することができる長さ 12 ビットとして仮に設定される。

【表 1】

IPMP ツール ID リスト

| ツール機能          | IPMP ツール ID               | IPMP ツール名前      | 注                                   |
|----------------|---------------------------|-----------------|-------------------------------------|
| 暗号解読<br>ツール    | ... 0001 000000000000 ... | DESDecrypt      | 12 ビットにより<br>4096 の異なる<br>ツールが可能になる |
|                | ... 0001 000000000001 ... | AESDecrypt      |                                     |
|                | ... 0001 000000000010 ... | SC2000Decrypt   |                                     |
|                | ... 0001 000000000011 ... | CamelliaDecrypt |                                     |
|                | ... 0001 000000000100 ... | Xxxx            |                                     |
|                | ... 0001 000000000101 ... | Xxxx            |                                     |
|                | ... 0001 000000000110 ... | Xxxx            |                                     |
|                | ... 0001 000000000111 ... | Xxxx            |                                     |
|                | ... 0001 000000001000 ... | Xxxx            |                                     |
|                | ... 0001 00000000xxxx ... | Xxxx            |                                     |
|                | ... 0001 00000000xxxx ... | Xxxx            |                                     |
|                | ... 0001 100000000000 ... | 予約              | 今後／独占ツール<br>に予約                     |
|                | ... 0001 100000000001 ... | 予約              |                                     |
|                |                           |                 |                                     |
| 透かし埋め込み<br>ツール | ... 0010 000000000000 ... | 透かしツール 1        | 12 ビットにより<br>4096 の異なる<br>ツールが可能になる |
|                | ... 0010 000000000001 ... | 透かしツール 2        |                                     |
|                | ... 0010 000000000010 ... | 透かしツール 3        |                                     |
|                | ... 0010 000000000011 ... | Xxxx            |                                     |
|                | ... 0010 000000000100 ... | Xxxx            |                                     |
|                | ... 0010 00000000xxxx ... |                 |                                     |
|                |                           |                 | 今後／独占ツール<br>に予約                     |
|                |                           | 予約              |                                     |
|                |                           | 予約              |                                     |

注：上記の最初の 4 ビットはツールタイプ ID である

この表は端末に事前ロードされるべきであり、又は、端末は上記に示す標準化ツールID表に基づいて構築される。

位置識別子は転送機構を暗示し、1つのIPMPツールに関して2つ以上の位置識別子が可能である。IPMPツールマネージャは、前記識別子の各々を用いて前記ツールを検索しようと試みる。IPMPツールAの第1の位置識別子が成功した場合、次の位置識別子がスキップされ、さもなければ、第2の位置識別子に続く。

例えば、位置識別子は下記の様に記述される。

1. ローカル：端末システムの内部又は周辺装置

2. 外部：指定された端末システムの外部（http：，ftp：）

IPMPツール識別子は、2つの部分（位置タイプ及び位置詳細）から成る。位置タイプは、次のうちの1つでなければならない。位置タイプと位置詳細との間の対応は、表2に示されている。

【表2】

可能な位置タイプとそれらの詳細

| 位置タイプID | 位置タイプ          | 位置詳細                    |
|---------|----------------|-------------------------|
| 0000    | “ローカル”         | N/A                     |
| 0001    | “周辺装置”         | N/A                     |
| 0010    | “遠隔ダウンロード可能”   | Website (http, ftp ...) |
| 0011    | “遠隔ダウンロード不可能”  | Java servletなどの遠隔位置     |
| 0100    | “コンテンツストリーム内部” | この部分はIPMPツール自体を含むべきである  |
| ...     | ...            | ...                     |
| 1***    | 予約             | 予約                      |

ツールフォーマットIDは、IPMPツールID及びツール位置IDと共に伝送され、通知するのに8ビットを用いており表3に明記されている。

提供されたIPMPツールが何れのバイナリフォーマットであるかをIPMP端末は、DLL、JBC、又はその他などのツールフォーマットIDから知り、前記IPMP端末は、そのOSと合致する適切なフォーマットで前記ツールをダ

ウンロード又は検索できる。

【表 3】

ダウンロードされた I PMP ツールのフォーマット I D

| 8 ビット    | ダウンロードされたフ<br>ォーマット      | 対象プラットフ<br>ォーム            | コンパイラ                    | I PMP 端末                                 |
|----------|--------------------------|---------------------------|--------------------------|--|
| 00000000 | JBC<br>(Java バイト<br>コード) | JVM インタプリ<br>タ埋め込みマシ<br>ン | Java コンパ<br>イラ           | 殆どの携帯電話及<br>び STBs                       |
| 00000001 | DLL1                     | Windows マシン               | Microsoft<br>C コンパイ<br>ラ | Windows 上で実行<br>中の全 PC                   |
| 00000010 | DLL2                     | Unix マシン                  | gcc 及び他<br>のコンパイ<br>ラ    | 全 Unix, Linux OS                         |
| 00000011 |                          |                           |                          |  |
|          |                          |                           |                          |  |
| 予約       | DLL-AM33                 | パナソニックの<br>チップ            | AM33 コン<br>パイラ           | チップ依存の製造<br>に予約、及び特定<br>のコンパイラを必<br>要とする |
| 予約       |                          |                           |                          |  |
| 予約       |                          |                           |                          |  |
| 予約       |                          |                           |                          |  |
|          |                          |                           |                          |  |

5      ダウンロードされる I PMP ツールのツールフォーマット I D を定義して端末相  
互運用性を達成する目的は、次の通りである。

1      最近、殆どの携帯電話及び DTV STB は、J a v a 仮想マシン (J V  
M) で構築されており、ストリーム内の保持又は URL からのダウンロードを介  
して I PMP ツールを J a v a バイトコードにコンパイルして端末にダウンロー  
10      ドすることができる。

2      DLL は、P C 又は U n i x で使用される非常に普及しているフォーマット  
である。異なるビット数のフラグを使用して、ユーザの端末が何れの DLL フォ  
ーマットをダウンロードする必要があるかを通知する。

3 JVMも標準C/C++コンパイラも有しない他の端末に関して、例えば、あるDTV STBに、IPMPツールを、それらのコンパイラを用いてプリコンパイルしブロードキャストストリーム又は裏チャンネルを介してダウンロードすることができる。これは、放送業者又は製造業者がそれらのソフトウェアを更新  
5 したい時に現在DTV STBが行っていることである。

この場合、前記表の同じ予約ビットフラグを、放送業者と製造業者の両方により選択及び参照して、前記業者がIPMPツールの何れのフォーマットを検索して使用することができるかをDTV STBに通知する。

IPMPツールリスト用構文は、次の通り定義される。

10 **【数1】**

```
class IPMP_Tool_List
{
    bit(128) IPMP_Tool_ID;
    //whether this IPMP Tool is a parametric tool or normal tool is
15 implicitly
    // indicated by the IPMP_Tool_ID.
    if (parametricRepresentation)
    {
        //... detailed syntax of parametric representation.
20     }
    else
    {
        bit(1) hasAlternativeToolLocation;
        while (hasAlternativeToolLocation)
25     {
            bit(1) hasAlternativeToolLocation;
            bit(7) Tool_Location_ID;
            if (Tool_Location_ID == 0b00000000) //tool carried in
                bitstream.
```



14

```

    {
    }
    else if (Tool_Location_ID == 0b0000001) //remote method
call
5      {
        bit(8) Remote_Call_Mechanism; //CORBA, DCOM, RMI,
        //SOAP ...
        bit(1) Client_In_Bitstream;
    }

10      else if (Tool_Location_ID == 0b0000010 ||
Tool_Location_ID=0b0000011)
        // Remote Downloadable, http protocol or ftp
        protocol
        {
15          bit(8) Tool_Format_ID;
          unsigned int(16) serverAddressLen;
          bit(8) serverAddress[serverLen];
          unsigned int(16) fullPathLen;
          bit(8) fullPath[fullPathLen];
20          bit(1) isCompressed;
          if (isCompressed)
          {
              bit(7) compressionMethod;
          }
25      }

    else if (Tool_Location_ID == 0b0000100 .. 0b1000000)
//ISO reserved
    {
    }

```

15

```

        else // user defined.
        {
        }
    }
5      }
    }
}

```

### 意味

IPMP\_\_Tool\_\_IDは、ユニバーサルレベルでツールを一意に識別する。最初の16ビットは特定のIPMPツールのタイプカテゴリを識別するのに対し、次の112ビットは前記IPMPツールを詳細に識別する。下記の表に、前記IPMP\_\_Tool\_\_IDを説明する。登録当局が、そのような表を保守する責任を持つ。

幾つかの通常用いられるIPMPツールを標準化する必要がある、それらの基本的なIPMPツールを含むテーブルを定義する必要がある、このテーブルをあらゆるIPMP端末に事前ロードするべきである。下記の表はこの考えを説明する。標準化されるべき基本ツールの内容に関して、それはIPMP委員会で更に論議する事項である。

Tool\_\_Location\_\_IDは、転送機構を暗示し、ツールがコンテンツストリームに保持されるか、遠隔位置からダウンロードする必要があるか、又はIPMPツールが遠隔位置で実行可能であるか否かを示す。

1つのIPMPツールに関して2つ以上の位置識別子が可能である。hasAlternativeToolLocationは、IPMPツールがべつの検索先を有するか否かを示す。IPMPツールマネージャは、前記識別子の各々を用いて前記ツールを検索しようと試みる。IPMPツールAの第1の位置識別子が成功した場合、次の位置識別子がスキップされ、さもなければ、第2の位置識別子が調べられる。

【表 4】

I P M P ツール位置識別子 (I P M P   T o o l \_ L o c a t i o n \_ I D)

| Tool_Location_ID     | 位置タイプ                  |
|----------------------|------------------------|
| 000 0000             | コンテンツストリームの内部に保持されたツール |
| 000 0001             | 遠隔位置で実行されるツール          |
| 000 0010             | httpプロトコルによるダウンロード     |
| 000 0011             | ftpプロトコルによるダウンロード      |
| 000 0100 -- 100 0000 | ISO予約                  |
| 100 0001 -- 111 1111 | 予約                     |

T o o l \_ L o c a t i o n \_ I D が 0 b 0 0 0 0 0 0 0 0 である場合、それは、  
 5 I P M P ツールがコンテンツストリームに保持されていることを意味する。M p  
 e g 4 データにおいて、本発明では、I O D と関連のある提案された I P M P ツ  
 ール E S 内にバイナリ I P M P ツールを入れる。その詳細は、後で説明する。

T o o l \_ L o c a t i o n \_ I D が 0 b 0 0 0 0 0 0 0 1 である場合、それは、  
 この I P M P ツールが遠隔側で実行されるものであることを意味し、I P M P 端  
 10 末は、R P C (遠隔手続き呼び出し) を介してこの I P M P ツールを呼び出す。

8 ビット遠隔呼び出し方法は、この I P M P ツールが何れの R P C 機構、例えば  
 C O R B A 、R M I 、X M L - R P C 、D C O M に対応しているかを示す。この  
 R e m o t e \_ C a l l \_ M e c h a n i s m に関する詳細は、下記の表で定義  
 される。I P M P ツールマネージャは、前記端末が前記 R P C 機構に対応してい  
 15 るか否かをチェックする。

【表 5】

I P M P   R e m o t e \_ C a l l \_ M e c h a n i s m

| Remote_Call_Mechanism  | RPC機構   |
|------------------------|---------|
| 0000 0000              | DCOM    |
| 0000 0001              | RMI     |
| 0000 0010              | CORBA   |
| 0000 0011              | XML-RPC |
| 0000 0100              | SOAP    |
| ... ..                 | ... ..  |
| 0000 1000 -- 1000 0000 | ISO予約   |
| 1000 0001 -- 1111 1111 | 予約      |

前記 I P M P ツールが遠隔で実行されるものである場合、I P M P 端末は、遠隔 I P M P ツールとインタフェースをとって通信するクライアントのような軽量コードを必要とする。例えば、前記遠隔 I P M P ツールが C O R B A を介して呼び出されることができるだけである場合、前記 I P M P 端末は、I I O P (インターネット O R B 間プロトコル) を介して前記遠隔 I P M P ツールに適切にパラメータをひとまとめに伝達する方法を知っているスタブを必要とする。本発明では、この軽量バイナリコードを I P M P ツールクライアントとして呼び出す。I P M P ツールクライアントは軽量であると考えられているので、それは可能であり、コンテンツストリーム内に保持される。この I P M P ツールクライアントをコンテンツストリーム内に保持する方法は、後で説明する。

遠隔で実行される I P M P ツールと通信する I P M P ツールクライアントを有するだけでは、I P M P 端末がこの遠隔 I P M P ツールを利用することを可能とするのに十分でない。I P M P 端末は、前記 I P M P ツールクライアントを初期設定してそれに話しかける方法を必要とする。これを処理する方法は、この提案の範囲外である。この面において、I P M P ツールクライアントは他の通常の I P M P ツールと同じように見える。従って、前記 I P M P ツールを丁度他の I P M P ツールのように初期設定して呼び出すべきであり、例えば、I P M P ツールクライアントと I P M P 端末との間のインタフェース定義は、この I P M P ツールクライアントが動作することになっている O D 又は E S D 間の I P M P 記述子に保持されても良い。

Tool\_Location\_IDが0b0000010である場合、それは、  
 IPMPツールマネージャがhttpプロトコルによって特定のIPMPツール  
 をダウンロードすべきであることを意味する。0b0000011は、ftpプ  
 ロトコルを使用すべきであることを意味する。ServerAddress（例  
 5 えば、www.panasonic.com）及びfullpath（例えば、  
 /ipmptools/encryption/tool1.zip）は、この  
 特定のIPMPツールを検索する場所をはっきりと定義する。IPMPツールマ  
 ネージャがhttp又はftpプロトコルを実施して必要なIPMPツールを検  
 索する方法は、本発明の応用課題である。特定のIPMPツールを検索するの  
 10 使用可能な複数種のプロトコル（https、ssl）がある場合もある。ISO  
 予約ビット範囲0000100ー1000000は、複数種のプロトコルを  
 保持する様に設計されている。

IPMPツールプロバイダがそれ自身の独占プロトコルを使用したい場合には、  
 ビット範囲1000001ー1111111を使用すれば良い。

15 IsCompressedビットは、指定ツールが圧縮されているか否かのフ  
 ラグを立てる。圧縮されている場合、IPMPツールマネージャは、compressionMethod欄に明示の圧縮方法に従って前記ツールを伸張する必  
 要がある。PC用圧縮方法は多数あり、とりわけPKZip、LHArc、AR  
 J、及びZOOがある。マッキントッシュでは、StuffIt、Compact  
 20 tPro及びその他がある。複数の圧縮方法をIPMPで使用できる様にするこ  
 ともでき、又は1つの圧縮方法をデフォルトとして指定することもできる。

#### IPMP\_\_ToolES

25 Mpeg4システムのデータにおいて、本発明では、基本ストリーム間に（前  
 記で提案したIPMPツールクライアントを含む）バイナリIPMPツールを保  
 持する。その目的を果たすために、本発明では、基本ストリームに対応付けられ  
 たデコーダ構成記述子に新しいストリームタイプを定義する。

ストリームタイプ“IPMPToolStream”を以下の様に、提案する。  
 0x0Aー0x1FがISO使用のために予約されているので、このストリーム  
 タイプに割当てられる値を0x0Aと設定する。従って、Mpeg4システム仕

様の現バージョンで定義されたストリームタイプ表を、下記のように変更する。

【表 6】

IPMP Remote\_Call\_Mechanism

| ストリームタイプ値   | ストリームタイプ記述                                   |
|-------------|--|
| 0x00        | 禁止   |
| 0x01        | ObjectDescriptorStream (ISO/IEC 14496-1 参照)  |
| 0x02        | ClockReferenceStream (ISO/IEC 14496-1 参照)    |
| 0x03        | SceneDescriptionStream (ISO/IEC 14496-1 参照)  |
| 0x04        | VisualStream                                 |
| 0x05        | AudioStream                                  |
| 0x06        | MPEG7Stream                                  |
| 0x07        | IPMPStream (ISO/IEC 14496-1 参照)              |
| 0x08        | ObjectContentInfoStream (ISO/IEC 14496-1 参照) |
| 0x09        | MPEGJStream                                  |
| 0x0A        | IPMPToolStream                               |
| 0x0B - 0x1F | ISO 使用に予約                                    |
| 0x20 - 0x3F | ユーザ専用  |

- 5 前記 IPMPToolStream を復号するデコーダは、IPMP ツールマネージャである。0x0A のストリームタイプを参照する際に、IPMP 端末は、構文解析する IPMP ツールマネージャに前記基本ストリームを渡す。IPMPToolStream は、初期オブジェクト・デスク립タ OD に通常置かれている。

10 IPMP\_\_ToolES の構文

【数 2】

```
class IPMP_ToolES
{
    IPMP_Tool ipmp_tools[0 .. 255];
}
```

```
class IPMP_Tool
{
    bit(128) IPMP_Tool_ID;
```

```

        bit(8)  Tool_Format_ID;
        bit(1)  isCompressed;
        if (isCompressed)
        {
5             bit(7)  compressionMethod;
        }

        bit(1)  isSigned;
        if (isSigned)
10     {
            bit(8)  signature_Algorithm[];
            bit(8)  signature_Parameters[];
            bit(1)  IPMP_Tool_List_Signature[];
        }
15     bit(16) Tool_Size;
        bit(Tool_Size) Tool_Body;
    }

```

IPMP\_\_ToolESの意味

20 IPMP\_\_Tool\_\_ID、Tool\_\_Format\_\_IDは、前記で定義されている内容と同じ意味を有する。

前記基本ストリームに保持されたIPMP\_\_Toolは、IPMP\_\_Toolの保全性を保証するのにある特定の署名アルゴリズムを用いて署名可能である。

前記署名の確認後、IPMPツールマネージャは、Tool\_\_Sizeにより指定されたサイズのTool\_\_Bodyをハードディスク又は物理メモリに適切  
25 に格納する。前記端末又はメッセージルータは、そのことを認識している。

前記IPMPToolStreamに保持可能なIPMPツールは、提案したIPMPツールクライアントを含む。基本ストリームからの検索及びIPMP端末による初期設定の後、IPMPツールクライアントは、遠隔IPMPツールと対話する。しかし、前記端末にとって、前記IPMPツールクライアントは、一

意の I P M P \_ T o o l \_ I D を有する通常の I P M P ツールとあまり変わらない。

### 1. 3 I P M P ツールマネージャ

I P M P ツールマネージャは、システムのデマルチプレクサの前又は後に位置  
5  
することができる。その機能性は、コンテンツストリーム内にある I P M P ツール  
リストを構文解析することである。

図 4 に示す線図は、I P M P ツールマネージャが M p e g 4 - I P M P システム  
に組み込まれた例を示す。

I P M P ツールマネージャは、次の 4 つのステップを実行する。

- ・ステップ 1 : 入力 I P M P データを I P M P ツールリストを求めて構文解析す  
10  
る。前記リストがない場合、ステップ 4 に進み、他の場合、正規の構文に従って  
前記 I P M P ツールリスト間の I P M P ツール情報を構文解析する。
- ・ステップ 2 : すべての要求 I P M P ツールが端末に入手できる場合、ステップ  
4 に進む。
- ・ステップ 3 : I P M P ツール情報で指定された必要な I P M P ツールを検索し、  
15  
検索が成功しない場合、中止し、他の場合、ステップ 4 に進む。
- ・ステップ 4 : 全 I P M P ツールをうまく取得した後、アクセス許可がある場合、  
利用可能なコンテンツは、データバッファに流れ始めることが可能となる。

コンテンツストリームを受信する際に、I P M P ツールマネージャは、あらゆる  
コンテンツストリームに関する一意のヘッダである I P M P ツールリストパケ  
20  
ットフラグを捜すことにより前記コンテンツストリームをまず調べる。I P M P  
ツール情報パケットの前記フラグが見つからない場合、ステップ 4 にジャンプす  
る。

第 3 のステップにおいて、I P M P ツールマネージャは、位置識別子タイプ I  
D 及び位置識別子詳細を調べることにより各 I P M P ツールを検索しようと試み  
25  
る。1 つの I P M P ツールに対応付けられた 2 つ以上の位置識別子がある場合、  
前記 I P M P ツールマネージャは、まず位置識別子 1 を用いて前記 I P M P ツール  
を検索しようと試み、それが失敗した場合、次に位置識別子 2 を用いて検索し  
ようと試みる。

位置識別子タイプが「ローカル」の場合、I P M P ツールマネージャは、指定



された I PMP ツール名前又は I PMP ツール I D に従って端末自身の中を探索する。

位置識別子タイプが「周辺装置」の場合、I PMP ツールマネージャは、指定された I PMP ツール名前又は I PMP ツール I D に従ってすべての周辺装置を探索する。

位置識別子タイプが「遠隔ダウンロード可能」の場合、I PMP ツールマネージャは、指定された遠隔アドレスに接続し、必要ならば、相互に受入れ可能な通信チャネルを I PMP ツールマネージャとツールプロバイダとの間にセットアップする。

位置識別子タイプが「遠隔ダウンロード不可能」の場合、I PMP ツールマネージャは、前記遠隔アドレスを I PMP システムに渡すだけである。

位置識別子タイプが「コンテンツストリーム内部」の場合、I PMP ツールマネージャは、ツールフォーマット I D をチェックすることにより端末に適合するバイナリフォーマットで前記ツールをロードし、ツール記述子として格納されたツールエンティティに I PMP ツール I D を割当てて。

デマルチプレクサインターフェース 304 の後に、音声デコーダバッファ 306、映像デコーダバッファ 307、I PMP ツールデコーダバッファ 301、オブジェクトディスクリプタデコーダバッファ 308、バイナリデータフォアシーン

(binary data for scene) (B I F S) デコーダバッファ 309、I PMP デコーダバッファ 310 が含まれる。バイナリデータフォアシーンは、セグメント化されたシーンの配置場所を示すデータが含まれる。306, 307, 309 の出力である、音声信号、映像信号、B I F S 信号はまだ暗号化されたままの状態である。メモリ 302 にはツール A (一つ、又は複数) が各端末に予めインストールされている。

音声デコーダバッファ 306 は制御ポイント 331 を介して音声復号 311 に接続され、映像デコーダバッファ 307 は制御ポイント 332 を介して映像復号 312 に接続され、オブジェクトディスクリプタデコーダバッファ 308 は、そのままオブジェクトディスクリプタ復号 313 に接続され、バイナリデータフォアシーン (binary data for scene) (B I F S) デコーダバッファ 309 は制御

ポイント 3 3 3 を介して B I S F 復号 3 1 4 に接続される。また、I P M P デコーダバッファ 3 1 0 は、I P M P メッセージルータ 3 2 4 の I P M P エレメンタリーストリーム 3 2 5 に接続される。I P M P エレメンタリーストリーム 3 2 5 には暗号化されたスクランブルキーが保持されている。

- 5 図において、黒丸で示された制御ポイント 3 3 1 ~ 3 3 9 は、I P M P 制御ポイントであり、制御ポイントを通過するデータは、I P M P システム 3 2 4 にあるツールを利用して、必要な処理（デスクランブル、透かし検出、コピーガード等）が加えられる。

- 10 この実施の形態では、制御ポイント 3 3 1, 3 3 2, 3 3 3 ではデスクランブルが行なわれる。デスクランブルに必要なツール（ソフト）は、I P M P メッセージルータ 3 2 4、端末ツールメッセージインターフェース 3 2 1 を介して I P M P ツール 1、2、又は 3 から取得する。

- 15 音声復号 3 1 1 は、制御ポイント 3 3 4 を介して音声コンポジタバッファ 3 1 5 に接続され、映像復号 3 1 2 は、制御ポイント 3 3 5 を介して映像コンポジタバッファ 3 1 6 に接続され、B I F S 復号 3 1 4 は、制御ポイント 3 3 6 を介して復号 B I F S 3 1 7 に接続される。

- 20 制御ポイント 3 3 4, 3 3 5, 3 3 6 では透かし検出が行なわれる。透かし検出に必要なツール（ソフト）は、I P M P メッセージルータ 3 2 4、端末ツールメッセージインターフェース 3 2 1 を介して I P M P ツール 1、2、又は 3 から取得する。例えば、I P M P ツール 2 は、デスクランブルに必要なツールが保持されており、I P M P ツール 3 は、透かし検出に必要なツールが保持されている。

- 25 音声コンポジタバッファ 3 1 5 は、制御ポイント 3 3 7 を介して合成器 3 1 8 に接続され、映像コンポジタバッファ 3 1 6 は、制御ポイント 3 3 8 を介して合成器 3 1 8 に接続され、復号 B I F S 3 1 7 は、制御ポイント 3 3 9 と B I F S ツリー 3 1 9 を介して合成器 3 1 8 に接続される。合成器 3 1 8 は更に出力であるレンダリング 3 2 0 に接続される。

制御ポイント 3 3 7, 3 3 8, 3 3 9 では別の透かし検出や、コピーガード処理が行なわれる。透かし検出やコピーガード処理に必要なツール（ソフト）は、

I PMPメッセージルータ 3 2 4、端末ツールメッセージインターフェース 3 2 1 を介して I PMP ツール 1、2、又は 3 から取得する。

I PMP ツールマネージャ 3 0 0 は、I PMP ツールリストを解析する解析部 3 5 0 と、I PMP ツールを検索する検索部 3 5 1 がある。オブジェクトディスクリプタデコードバッファ 3 0 8 は、そのままオブジェクトディスクリプタ復号 3 1 3 に接続され、コンテンツストリームに含まれるオブジェクトディスクリプタを復号する。復号されたオブジェクトディスクリプタは、I PMP ツールマネージャ 3 0 0 に送られ、必要とされるツールが存在する位置について特定がなされ、そのツールを取得するためのデータが I PMP ツールマネージャ 3 0 0 から ツールメッセージインターフェース 3 2 1 に送られる。ツールメッセージインターフェース 3 2 1 は、特定されたツールがメモリ 3 0 2 にあればそのツールを I PMP ツール 2 または 3 に移動し、必要な処理を行なう。特定されたツールがメモリ 3 0 2 にない場合は、インターネットなどの伝送路を介し、リモートツール 3 6 0 にアクセスし、必要なツールを I PMP ツール 1 にダウンロードする。また、必要なツールが遠隔 I PMP ツール B 3 6 2 にしかなく、ダウンロードが出来ない場合は、暗号化されたデータをそのまま、I PMP ツール B のローカルクライアント 3 6 4 を介して遠隔 I PMP ツール B 3 6 2 に送り、遠隔 I PMP ツール B 3 6 2 で解読したデータを送り返す様に動作する。

I PMP ツールマネージャ及び I PMP ツールリストを含むこのアーキテクチャは、任意の MPEG-n システムに適用でき、図 5 は、I PMP ツールマネージャが MPEG 2-I PMP システムに組み込まれる場合を示す。ここに示す例では、オブジェクトが含まれない。PES で示される黒丸で示す制御ポイントにおいてデスクランブルや、透かし情報の解読が行なわれる。

コンテンツの同一部分に対しては、MPEG-n の I PMP システムに関する一般的な構文は、次のような流れで定義可能である。

### 【数 3】

```
Class   UserAuthentication( )
{
    Class   ReceivingContentStream( )
```

```

{
    Class      DemuxContent( )
    {
        Class  IPMPToolsManagement( )
5           {
                Class ParseIPMPToolsInformation( ); //IPMP Tool
                Management module, see 2.3 for details;
                Class RetriveIPMPTools( );           //IPMP
10              Tool Management module, see 2.3 for
                details;
                {
                    Class      ContentConsumptionStart( );
                }
            }
15        }
    }
}

```

## 2. ユーザ権利認証に指定されるべき出力メッセージ

ユーザ権利認証（RA）方法を標準化することは勧められていないけれども、  
 20 認証結果又はRA用出力メッセージは、基準を定めたり、又は予め定める必要が  
 ある。このメッセージは、保護コンテンツの許可使用のためにMPEG-nのI  
 PMPシステムを通過する必要がある。

我々は、認証出力メッセージを標準規格として設定すべきであることを提案し、  
 その標準は、下記のように少なくとも3つのフィールドから成るべきである。

### 25 【表 7】

|              |       |       |   |
|--------------|-------|-------|---|
| 有効性<br>(真/偽) | ライセンス | 利用ルール | 空 |
|--------------|-------|-------|---|

ユーザ権利認証（RA）の機能に関する構文は、次の通りリストされる。

## 【数 4】

```

Class   RightAuthenticationMessages( )
{
    bit(1) Valid;
5      if(valid)
    {
        Class   RetrieveLicence( );
        Bit(16) Licence;
        Class   UsageRule( );
10      Bit(length)   UsageRule;
    }
}

```

妥当性は、ユーザ（端末）が正当であるか否かを示し、その結果は単なる真又は偽の表示でもよい。使用規則は、コンテンツにアクセスするユーザ権利の詳細
 15 を含むべきである（例えば、1回又は複数回のプレー）。ライセンスは、以下に説明する。

I P M Pデータに示すように（例えば、M p e g 4－I P M PのI P M P－E S）、コンテンツにスクランブルがかけられ、そのスクランブルキーをコンテンツストリーム内に伝送することが知られている。例えば、I P M P－E Sには暗
 20 号化されたスクランブルキーが入っている。より高いセキュリティを確保するために、前記スクランブルキーは、2層のセキュリティを達成するよう更に暗号化可能である。スクランブルがかけられているコンテンツ用のスクランブルキーを暗号解読するのに使用される第2層のキーは、「ライセンス」と呼ばれる。「ライセンス」は、保護コンテンツを消費する最小要件である。ライセンスは、非基
 25 準ユーザ認証処理の間に安全なチャネルを介してライセンスサーバから検索されるべきである。

上記認証出力メッセージは、たとえI P M P端末がどんな種類のユーザ認証方法を使用しても、ユーザ認証中に提供されて出されるべきである。

ここで使用規則は、消費タイプ及び規則用のバイナリフォーマットに関する表

4で更に定義可能である。代わりに、前記使用規則を、バイナリフォーマットではなくXMLフォーマットで定義して対話することもできる。

【表 8】

バイナリフォーマットで定義された消費タイプ及び規則

| 消費タイプ         | 8 ビット    | 消費規則タイプ<br>4 ビット+変数 | 注         |
|---------------|----------|---------------------|-----------|
| アクセス          | 00000000 |                     | アクセスコンテンツ |
| プレー (ストリーミング) | 00000001 |                     | ストリーミング再生 |
| 格納及びプレー       | 00000010 |                     | 格納及び再生    |
|               |          | 0001 + プレーカウント      |           |
|               |          | 0010 + プレー時間        |           |
|               |          | 0011 + プレー期間        |           |
|               |          | 0100 + コピーカウント      |           |
|               |          | 0101 + 移動カウント       |           |
|               |          | 予約                  |           |
| シーングラフ編集      | 00000011 |                     |           |
| 時間ライン編集       | 00000100 |                     |           |
| テキスト又はその他の追加  |          |                     |           |
|               | 予約       |                     |           |
|               |          |                     |           |

5

図 6 に示す線図は、MPEG-4 の IPMP システムと共に作動するユーザ認証モジュールを示し、ユーザ認証の実行後にコンテンツエージェントを要求してライセンスをユーザに発行する。ユーザ ID 情報は、IPMP システム内に含まれている。このユーザ ID 情報が標準では定義しないユーザ認証においてユーザ ID の照合が行なわれる。この照合には例えば乱数が用いられる。照合が成立すれば、正しいユーザとしてサーバに対しユーザ登録を行なう。

10

図 7 の線図に示すように、2重セキュリティ構造は、MPEG-n の IPMP に関して実現可能である。サーバから送られてきたライセンスキーは、IPMP ツール保持部に送られる。また、コンテンツストリームに含まれる暗号化されたスクランブルキーが点線で示す経路を経て、IPMP ツール保持部に送られる。IPMP ツール保持部では、ライセンスキーを用いてスクランブルキーの解読を行なう。解読されたスクランブルキーは、スクランブルキー保持部で保持され、

15

I PMPツールの動作に使用される。この様に、I PMPツールは、スクランブルキーとライセンスキーによる2重のセキュリティがかかっている。

### 3. I PMPツール用の一般的なインタフェース

データ暗号化／暗号解読、透かし、及び結合透かし及び暗号解読を使用する典型的な用途シナリオを我々が設定した場合、汎用のインタフェースを定義することができる。

#### データ検出インタフェース

ブロックベースデータ暗号化／暗号解読ツールは、独自のI PMPシステムにおいてより重要でより広く使用され、特にそのアルゴリズムはある種の収束性を有することが知られている。そこで、そのインタフェースをうまく指定してデータ暗号化及び暗号解読技法の殆どを表すことができ、前記技法の一部は知られていないが、そのインタフェースは予測範囲内である。

#### データ暗号化／暗号解読の対称アルゴリズム用のNESSIEインタフェース

あらゆるアクセスユニットのブロックベースデータ暗号化／暗号解読用の汎用インタフェースは、I PMPシステムで定義可能である。I PMPツールプロバイダとI PMP端末実施者の両方は、同一のインタフェースに従って、ツールプロバイダ側でツールをバイナリフォーマットにコンパイルし、I PMP端末側に正しいバイナリツールを伝達することができる。下記のインタフェースは、NESSIE（署名、保全性及び暗号化に関する新欧州方式）で定義されており、我々は、ブロックデータ暗号化／暗号解読用に我々が定義したI PMPシステムで前記インタフェースに適合することができる。前記インタフェースは、下記のように示され、3種類、NESSIEkeysetup（ ）、NESSIEencrypt（ ）及びNESSIEdecrypt（ ）から成る。

```
void NESSIEkeysetup(const unsigned char * const key, struct NESSIEstruct
* const structpointer);
```

```
void NESSIEencrypt(const struct NESSIEstruct * const structpointer,
const unsigned char * const plaintext, unsigned char * const
ciphertext);
```

```
void NESSIEdecrypt(const struct NESSIEstruct * const structpointer,
```

```
const unsigned char * const ciphertext, unsigned char * const
plaintext);
```

#### 透かしインタフェース

透かしを使用する目的に関して、4つの主な分野がある。

- 5     ・著作権保護——メディアデータの正当な所有権を決定する。
- ・違法コピー追跡——違法製造コピーを監視して追跡する。
- ・コピー保護——メディアの許可されていないコピーを禁止する。
- ・画像認証——データの改造を検出する。

10     前記分野の各々を分析することにより、次のような事が分かる。著作権保護の場合、符号化側で埋め込みを行い、オフラインで検出を行う。そこでは、他のリアルタイム暗号解読及び復号モジュールと共に I P M P 端末で実時間実施される必要はない。

コピー保護の場合には、透かしの使用よりも権利認証ツールの方がずっと複雑な使用規則を提供できるので、よりうまく処理可能である。

15     コンテンツ暗号化及び復号を制御する透かしを使用する場合、透かし検出器は、I P M P 端末で指定して実装する必要がある。

たとえ透かしコピー制御埋め込み及び検出にどんなアルゴリズムを使用しても、透かし検出用の汎用インタフェースは、次の通り準拠 I P M P 端末に関して指定可能である。

20     P S L 透かし検出 (Unsigned Char\* Input, Unsigned Char\* WatermarkInfor)

コピー制御をコンテンツプロバイダ／ディストリビュータ側で埋め込み、暗号化及び復号後にコピー制御検出を行うので、上記インタフェースを、I P M P 端末で指定して実装することで、異なる透かし検出技法をも I P M P 端末で使用可能にする必要がある。

25     画像認証に関して、この場合は著作権保護と同様である。それは、オフラインで行うことができる。

違法コピー追跡用には、他のシステムで広く提案され使用されているコンテンツ追跡の目的でユーザ I D 又は端末 I D を埋め込む透かし埋め込みは優れた機能である。また、基本的な特徴として透かし埋め込みを使用することをここで提案



し、I PMPシステムに格納されたり再生用途でコンテンツが違法にコピーされるのを更に防ぐ。ここでI PMPシステムでは、良く知られているように、最初には保護がデータ暗号化／暗号解読を介して行われ、違法コピーに関する追跡が透かし埋め込みを介して行われる。

- 5        たとえ透かし埋め込み、空間定義域又は周波数定義域にどんな技術を使用しても、たとえそれらをどんな分野、映像又は音声に使用しても、入力メッセージ及び出力メッセージは同一であるべきであり、それは次の通りである。

PSLWatermarkEmbedding (Unsigned Char\* Input, Unsigned Char\*  
WatermarkInfor, Unsigned Char\* Output)

- 10        この場合、透かしの検出をオフラインで行うことができる。

どんな種類のアルゴリズムがユーザID又は端末IDの透かし埋め込みに使用されるかに関しては、I PMP端末実施者の責任である。この場合、準拠I PMP端末が透かし埋め込み機能を実施してID又は端末IDを埋め込み違法コピーを追跡する必要があるI PMPシステムで要件を設定する限り、前記インタフェースは、I PMPシステムで指定する必要さえもない。

15

I PMP端末で使用された独立型透かしに関する結論では、汎用インタフェースは透かしを用いたコピー制御検出の場合にのみ定義される。

結合透かし検出及びデータ暗号解読

- 20        コンテンツに埋め込まれる暗号解読用キーは、キー自体を処理することによりコンテンツを保護する優れた方法である。このような場合、2つのインタフェースを次の通り指定可能である。

PSLWatermarkExtraction(Unsigned Char\* Input, Unsigned Char\* Key)

PSLDecryption(Unsigned Char\* Input, Unsigned Char\* Key, Unsigned Char\*  
Output)

- 25        処理は、下記のようなものである。

AU用コンテンツ復号→キー抽出→前述のAUで抽出されたキーを用いた次のAU暗号解読、循環規則で実行可能である。

#### 4.    部分的データ暗号解読

図8では、データ暗号化及び暗号解読をビットストリーム全体ではなくビット

に適用して選択することができることを示している。

図 8 (a) では、エンコーダを有する部分的暗号化を示しており、コンテンツプロバイダ側で符号化処理中に重要なビットに関して暗号化を選択的に実行できることを説明する。

- 5 図 8 (a) において、モジュール 8. 1 は、MPEG 2、MPEG 4 などに基づいて音声又は映像などの元の入力源をストリームに符号化するエンコーダである。モジュール 8. 2 では、選択されたビット又は情報が他のビットの中で必須又は重要であるため、これらのビット又は情報を暗号化してコンテンツを保護する。8. 0 はスイッチであり、8. 8 はスイッチ 8. 0 を切りかえるセクタである。図 8 (a) では、セクタ 8. 8 は予め決められた周期または時間区分により切り替え信号を出力する。これにより、エンコーダの出力は決められた時間区分において暗号化がかけられ、他の時間は暗号化がなされない。

- 10 図 8 (b) では、エンコーダでエンコードされたデータの内、暗号化を重要なビットに関して選択的に実行できる例を示す。なお、エンコーダ 8. 1 はコンテンツディストリビュータの中にある場合だけでなく、コンテンツディストリビュータの外にある場合も含む。後者の場合であれば、コンテンツディストリビュータは、エンコードされたストリームを受け、それを配信する。これは、コンテンツディストリビュータが既存又はそれら自体の暗号化ツールを用いて符号化コンテンツを保護したい場合である。

- 20 図 8 (b) において、モジュール 8. 3 は、モジュール 8. 4 で実行される暗号化用の重要なビットを構文解析して選択するセクタを有する部分的デコーダである。エンコードされたストリームは、そのままスイッチ 8. 0 に送られると共に、部分的デコーダおよびセクタ 8. 3 にも送られる。部分的デコーダおよびセクタ 8. 3 は、エンコードされたデータをデコードし、重要なデータ部分、たとえば映像信号の場合、I-ピクチャーの部分やP-ピクチャーの部分を検出する。そして、重要なデータ部分が検出された時に、その部分に対応するエンコードストリームの区分を暗号器 8. 4 に送る様にスイッチ 8. 0 を動作する。このため、エンコーダ 8. 1 からの分岐点とスイッチ 8. 0 との間に必要な遅延部を設けても良い。部分的デコーダおよびセクタ 8. 3 は、入力されるエンコード

された信号を部分的にデコードしても良いし、全体をデコードしても良い。

図 8 (c) は、デコード側の構成を示す。ここでは、部分的暗号解読が示されている。I PMP 端末側で生じる、部分的暗号化ストリームの暗号解読を選択的に実行する実施の形態を示す。

- 5        図 8 (c) において、モジュール 8. 5 は、モジュール 8. 6 で実行される暗号解読用のビットを構文解析して検出する検出器を有する部分的デコーダである。同時に、復号された音又は画像は、モジュール 8. 7 から出力される。検出器 8. 5 は、デコードを試みることにより、デコードが可能な部分と不可能な部分を検出する。不可能な部分については、その部分に相当するストリームは暗号化されている区分であると判断し、暗号化されている区分を検出する。ストリームの内  
10        暗号化されている区分は暗号解読器 8. 6 に送られ、暗号が解読される。

#### 5. I PMP システム用の可能なプロファイル

- 異なるアプリケーション、異なる端末、異なるベンダは、I PMP システムに関する異なる要件を有し、たった 1 つの基準で全部を扱うことは困難である。基本的  
15        的に、この課題は、I PMP ツールが事前ロードされるか、又はダウンロード可能であるかに依存する。単純なハードウェア実現に関しては、多くの場合が J a v a 仮想マシンを装備しているのである特定のツールがダウンロード可能であるセットトップボックスの新プラットフォームやモバイル装置でさえで多くの場合、殆どのツールは事前ロードされるか、又は組み込まれる。

- 20        複雑さの少ない実施を要求する場合にはので、あるモバイル又はポータブル端末は事前符号化 I PMP ツールを有する必要がある。P C アプリケーションは非常に柔軟であり、ツールは、ダウンロード可能又は事前符号化されていてもよい。

- I PMP ツールがダウンロード出来る場合、ダウンロードされた I PMP ツールのインタフェースも、定義される必要がある。メッセージインタフェースは、  
25        未知又は専用 I PMP ツールを処理する I PMP 端末に高い柔軟構造を与える優れた解決策であるが、I PMP 端末に対してより複雑な実装を要求する。

3 つのプロファイルを指定する場合、表 5 に示すように端末機能に基づいて 3 つの場合を扱う。すなわち、固定 I PMP ツール用の単純プロファイル、柔軟 I PMP ツール及び固定インタフェース用のコアプロファイル、並びに柔軟 I PMP

P ツール及び柔軟インタフェース用の高プロファイルの3つである。

【表 9】

異なる端末用の 3 つのプロファイル

| プロファイル                               | IPMP ツール取得 |                       |
|--------------------------------------|------------|-----------------------|
|                                      | 事前符号化      | ダウンロード済み              |
| 単純プロファイル<br>固定IPMPツール                | あり         | なし                    |
| コアプロファイル<br>柔軟IPMPツール及び固定インタフ<br>ェース | あり         | あり                    |
| 高プロファイル<br>柔軟 IPMP ツール及びインタフェ<br>ース  | あり         | あり、より多くのツールを<br>支援できる |

5 ツールが固定される場合は、標準の方法で勧められる IPMP ツールの種類を定義して製造者が端末に実装可能にする必要がある。この場合、インタフェースは、IPMP 端末実装者により決定される。

10 ツールは固定されないがインタフェースが固定される場合に関して、標準の方法で異種の IPMP ツールに関する幾つかの汎用インタフェースを指定する必要がある。

ツールとインタフェースの両方が固定されない場合に関して、メッセージインタフェースを詳細に指定して標準の方法で動作を通知する必要がある。

15 この発明は、IPMP ツールリストを構文解析して IPMP ツールを取得する IPMP ツールマネージャモジュールと共にコンテンツストリームの前の IPMP ツールリストパッケージを取り入れることにより異種の IPMP システムにより同一の保護コンテンツを再生する課題を解決する。IPMP ツールフォーマット ID を指定することにより、異なるフォーマットの IPMP ツールをダウンロードして IPMP 端末に一致させることができる。更に、3 つの主要な IPMP ツール用の一般的なツールインタフェースも、この発明で指定して IPMP システムを完全に  
20

2 層構造は、より高いセキュリティを与えるだけでなく、異なるユーザ認証方法用の出力構造も固定して、端末互換性を持たせる。このような構造では、ユー

ザ認証を異なるベンダに関して異なる方法で実施して、相互運用性を確保することができる。

異なるプロファイルは、I PMPツールを取得して使用する端末複雑性及び柔軟性を考慮して定義され、異なる端末及び異なるI PMPツールベンダに関して  
5 広範囲の適用を与えてながら同一の規準を使用することを可能にする。

図9は、他の実施の一例における著作権保護システムの構成図である。図9において、1はプロバイダ、2はユーザ端末、3はネットワークであり、プロバイダ1とユーザ端末2を接続している。プロバイダ1は、暗号化コンテンツ11と、その解読鍵12、及び、著作権保護ツールの一つである解読モジュール13と、  
10 著作権保護情報の一つであるコンテンツの利用規則14と、その利用規則を管理する著作権保護ツールの一つである利用規則管理モジュール15を持ち、ユーザ端末2は、初期状態としてなにも持っていない。

以上のように構成された本発明の一実施例における著作権保護（I PMP）システムにおいて、著作権保護システムを更新し、暗号化コンテンツを利用規則に従って解読、再生する方法を以下に述べる。  
15

図10は、本発明の実施例における著作権保護システムにおいて、プロバイダとユーザ端末の間で交換するメッセージの流れを示す図である。

図11は、メッセージの具体例であり、各メッセージは、「＝」記号の左辺に示す予め登録されているメッセージ項目名と、「＝」に続くメッセージ項目の値  
20 （データ）の組で構成される。

まず、ユーザ端末2は、視聴したいコンテンツを持つプロバイダにユーザ登録をして必要な著作権保護（I PMP）ツールを入手するためにメッセージ1をプロバイダ1へ送る。メッセージ1は、メッセージ項目として、メッセージID  
（識別子）、ユーザ名、支払い方法、及び、ユーザ端末情報より構成される。各  
25 メッセージ項目の値は以下である。メッセージ1の目的は、ユーザ登録である為、メッセージIDの値は「ユーザ登録」を表わす値であり、登録に必要なユーザ名の値は、「松下 太郎」である。又、視聴するコンテンツの対価の支払い方法の値は、ユーザのクレジットカードの種類、番号、有効期限を含む暗号化された  
「クレジットカード番号」である。ユーザ端末情報の値は、Windows OS上で動く

マシンであるので「Windows OS」である。

これらの情報は、ネットワーク 3 の入り口で更に暗号化され、出口でその暗号が解読される。

暗号の方法は、公開鍵暗号方式や共通鍵暗号方式が用いられるが、この内容は、  
5 例えば、岡本他「現代暗号」産業図書、1997年に詳述されている。

メッセージ 1 を受け取ったプロバイダは、ユーザ名、解読されたクレジット番号を記録し、ユーザ ID 「XYZ」をユーザ端末 2 に割り当て、ユーザ端末 2 にメッセージ 2 を返す。メッセージ 2 は、ユーザがコンテンツを視聴するために必要な初期設定を行うもので、メッセージ ID の値は、「初期設定」であり、ユーザ  
10 ID の値「XYZ」と、プロバイダが持っているコンテンツの一覧表である「コンテンツリスト」を IPMP 情報の値として含み、又、暗号化コンテンツを解読する為の解読モジュールの識別子（解読モジュール ID）と、その存在する場所（ロケーション）を、IPMP ツール情報の値として含む。更に、コンテンツを利用規則に従って視聴させる為、利用規則管理モジュールの識別子（利用規則管理  
15 モジュール ID）とその存在する場所（ロケーション）を IPMP ツール情報の値として含む。このとき、解読モジュールと利用規則管理モジュールは、Windows マシンであるユーザ端末に直接組み込めるものが選ばれる。メッセージ 2 も、以降のメッセージも、ネットワーク 3 を通過する際に暗号化されることは、言うまでもない。

20 メッセージ 2 を受け取ったユーザ端末は、解読モジュール ID とそのロケーションで指定される解読モジュールと、同じく利用規則管理モジュール ID とそのロケーションで指定される利用規則管理モジュールを、ファイル転送などの手段で入手し、自身に著作権保護ツール（IPMP ツール）として組み込む。このファイル転送も又、暗号化されたファイル転送であり、他のユーザ端末は暗号解読  
25 の鍵を持たない為、モジュールを傍受したとしても解読できない。

次に、ユーザ端末 2 は、コンテンツリストから視聴を希望するコンテンツ 1 を選び、コンテンツ要求をメッセージ ID として持つメッセージ 3 をプロバイダに送る。メッセージ 3 は、更に、ユーザ ID として値「XYZ」を含み、コンテンツ情報として要求するコンテンツ 1 の ID を含む。

これを受けたプロバイダ 1 は、要求されたコンテンツ 1 の対価を、ユーザのクレジットカード番号を使ってクレジットカード会社に請求した後、暗号化コンテンツ 1 をユーザ端末 2 に送る為、メッセージ 4 を返す。メッセージ 4 は、メッセージ ID と、2 つの著作権保護 (IPMP) 情報、及びコンテンツ情報で構成される。メッセージ ID の値は「コンテンツ配信」であり、IPMP 情報の値は、要求されたコンテンツ 1 の利用規則 1 と、暗号化されたコンテンツ 1 の暗号を解く為の解読鍵 1 である。コンテンツ情報は、要求された暗号化コンテンツ 1 そのものである。解読鍵 1 は、公開鍵暗号方式で暗号化されてユーザ端末 2 に送られるので、このメッセージ 4 を第三者が傍受しても解読鍵の暗号を解読出来ず、コンテンツの漏洩は起こらない。

メッセージ 4 を受け取ったユーザ端末 2 では、先ほど組み込んだ利用規則管理モジュール 25 が、利用規則 1 を確認しながら、解読モジュール 23 を制御し、解読モジュール 23 は、解読鍵 1 を使って、暗号化コンテンツ 1 を解読し、解読されたコンテンツ 1 を表示出力する。解読モジュール 23 が暗号化コンテンツ 1 の暗号を解く動作は、共通鍵暗号方式であり、上述の文献に詳しく述べられている。

次に、図 12 に示す利用規則 1 の一実施例に従い、暗号化コンテンツ 1 の解読を行う解読モジュール 23 を制御する利用規則管理モジュール 25 の動作を、図 13 のフロー図を用いて以下に説明する。

まず、利用規則管理モジュール 25 は、利用規則 1 の第 1 行目を調べ、このコンテンツが利用可能期間内に入っているか否かを、ユーザ端末の持つ時計で確認し、入っていなければ、処理を終了する。

入っていれば次に、ユーザにこのコンテンツを別メモリに移動するか否かを確認し、移動する場合は、利用規則 1 内の移動可能回数を調べ、この値がゼロより大であれば、ユーザの指定するメモリにコンテンツを移動し、移動可能回数を 1 減じる。

次に、ユーザにこのコンテンツのコピーを作るか否かを確認し、作る場合は、利用規則 1 内のコピー可能回数を調べ、この値がゼロより大であれば、ユーザの指定するメモリにコンテンツとその利用規則をコピーし、コピー可能回数を 1 減

じる。コピー先のコンテンツのコピー可能回数は、処理の簡単化のためにゼロとするが、トータルのコピー回数が初期のコピー可能回数を越えない様に制御しても良い。

次に、ユーザにこのコンテンツを再生するか否かを確認し、再生する場合は、  
5 利用規則1内の再生可能回数を調べ、この値がゼロより大であれば、解読モジュール23にコンテンツの解読・表示出力を指令する。

指令を受けた解読モジュール23は、コンテンツ1の暗号解読を行いその結果を表示出力することは上述の通りである。

次に、利用規則管理モジュール25は、再生終了を検出し、それまでに再生した時間が無料再生時間を超過したか否かを調べ、超過した場合は、再生可能回数を1減じて終了する。  
10

以上に述べた利用規則管理モジュール25による利用規則1の管理により、プロバイダ1が意図した回数の再生のみが実行される。同時に、コピー回数や、移動回数もプロバイダの意図どおりに管理される。

尚、本実施例では、メッセージは、予め決められたメッセージ項目と「＝」で結ばれたその項目の値（データ）との組で構成されていたが、メッセージの値の意味が分かる方法であれば何でも良く、例えば、メッセージ中のビットの位置に予め決められた意味を割り当てる方法でも良い。  
15

以上のような構成及び方法により、本発明の更新可能な著作権保護システムでは、プロバイダからユーザ端末に送られるメッセージをユーザ端末が解読することにより、著作権保護モジュールの更新と、プロバイダが与える利用規則に従ったコンテンツの視聴が可能となる。  
20

すなわち、メッセージ中にモジュールIDが存在するかしないかで、モジュールの更新を行うか否かが判定でき、モジュールIDが存在する場合はロケーションの値で、どこにモジュールがあるかが分かり、モジュールのダウンロードが可能となる。  
25

又、メッセージ項目名が予め決められているので、このメッセージ項目名を探すことで、メッセージ項目の値を得られるので、メッセージ項目とその値の組はメッセージ中にどの順番で入っていても良い。



又、上記の様に、プロバイダ 1 は、メッセージ 1 でユーザ端末 2 の OS の種類を知り、そのユーザ端末 2 に適合する著作権保護モジュール 1 を選んで、ユーザ端末 2 にダウンロードすることにより、ユーザ端末 2 は、仮想マシンを実装する必要はない。

## 請 求 の 範 囲

1. 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

5 データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化する手段と、

透かしツールを用いて当該コンテンツに透かし情報を埋め込む手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツ ID 及び I P M P (知的所有権管理保護) ツールリスト (I P M P ツール情報) を作成する手段と、

10

各コンテンツストリームのヘッダとして保持すべき I P M P ツールリストフラグを作成する手段と、

I P M P ツールリストフラグ、次いで I P M P ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

15

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I P M P システムの装置。

2. 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

20 データ暗号化ツール又は他のツールを用いた当該符号化コンテンツストリームを暗号化する手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツ ID 及び I P M P (知的所有権管理保護) ツールリスト (I P M P ツール情報) を作成する手段と、

25 各コンテンツストリームのヘッダとして保持すべき I P M P ツールリストフラグを作成する手段と、

I P M P ツールリストフラグ、次いで I P M P ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

3. 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

5 暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化する手段と、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化する手段と、

10 当該コンテンツストリームと同一のストリームに保持された I PMP 情報に上記当該暗号化されたキーを埋め込む手段と、

上記ステップで使われた当該コンテンツに関するコンテンツ ID 及び I PMP (知的所有権管理保護) ツールリスト (I PMP ツール情報) を作成する手段と、  
各コンテンツストリームのヘッダとして保持すべき I PMP ツールリストフラグを作成する手段と、

15 I PMP ツールリストフラグ、次いで I PMP ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

20 4. 請求項 1、2 及び 3 において当該コンテンツに関するコンテンツ ID 及び I PMP ツールリストを作成することが、

I PMP ツール ID を各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示する手段と、

25 位置タイプ ID を各 I PMP ツールに割当てて、当該 I PMP ツールが入手可能である位置のタイプを通知する手段と、

フォーマット ID を割当てて、ダウンロードされた I PMP ツールフォーマットを表示して、準拠 I PMP 端末がそれらのプラットフォームに基づいて選択及び検索することを可能にする手段と、

当該 I PMP ツールの位置を表示して、端末が当該 I PMP ツールを当該位置

から取得することを可能にする手段と、  
を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I P M P システムの装置。

5. I P M P 端末の I P M P ツールマネージャでコンテンツストリームの中を  
5 構文解析する手段と、

I P M P ツールリストフラグ、コンテンツ I D 及び I P M P ツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I P M P ツールリストに基づいて I P M P ツールを取得  
10 する手段と、

を含む、I P M P 端末側のコンテンツ提供及び保護用の柔軟 I P M P システムの装置。

6. I P M P 端末の I P M P ツールマネージャでコンテンツストリームの中を  
構文解析する手段と、

15 I P M P ツールリストフラグ、コンテンツ I D 及び I P M P ツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I P M P ツールリストに基づいて I P M P ツールを取得  
する手段と、

20 要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費の使用規則  
25 を取得する手段と、

を含む、I P M P 端末側のコンテンツ提供及び保護用の柔軟及び共通 I P M P システムの装置。

7. 要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証  
を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報を I PMP 端末で構文解析する手段と、

当該ライセンス又はキー情報を当該 I PMP 端末のメモリに格納する手段と、

5 当該 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析する手段と、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈する手段と、

10 ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得する手段と、

I PMP ツールリスト情報の当該部分と共に上記ステップで検索された当該 I PMP ツールを当該 I PMP 端末のメモリに格納する手段と、

15 当該メモリに格納された当該 I PMP ツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号する手段と、  
を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

8. 要求をコンテンツディストリビュータに送信して、ユーザ認証を行う手段と、

20 当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報を I PMP 端末で構文解析する手段と、

当該ライセンス又はキー情報を当該 I PMP 端末のメモリに格納する手段と、

25 当該 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析する手段と、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得

する手段と、

I PMP ツールリスト情報の当該部分と共に上記ステップで検索された当該 I PMP ツールを当該 I PMP 端末のメモリに格納する手段と、

5 当該ライセンス又はキー情報を用いて当該 I PMP 情報内の当該暗号化されたキーを暗号解読する手段と、

コンテンツプロバイダ側で当該コンテンツを暗号化するために使用された暗号化キーを上記ステップから取得する手段と、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得する手段と、

10 当該最初のコンテンツを当該 I PMP 端末での再生のために復号する手段と、を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

9. 請求項 5、6、7、8 のいずれかにおいて I PMP ツールリストは、

15 I PMP ツールの大部分に関する I PMP ツール ID をテーブル状に定義しており、

当該テーブルに予約可能な未使用スペースがあり、

I PMP ツールタイプとも呼ばれる I PMP ツールのカテゴリとして I PMP ツール ID の一部が定義されており、

20 当該テーブルを I PMP 端末に事前ロード、事前符号化又はダウンロードする手段と、

前記コンテンツストリーム内に保持された当該 I PMP ツールリストから当該 I PMP ツール ID を抽出する手段と、

前記コンテンツストリームに保持された当該 I PMP ツールリストに表示された I PMP ツール位置識別子を取得する手段と、

25 I PMP ツール位置識別子に加えて、I PMP ツール ID と共に、当該コンテンツストリームに保持された I PMP ツールフォーマット ID を取得する手段と、適切なフォーマットである I PMP ツールを選択して、I PMP 端末プラットフォームに適合させる手段と、

上記手段で取得された当該位置から当該 I PMP ツールを検索する手段と、

とを更に含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

10. 予め定めたテーブルに基づいて I PMP ツールリストを構築してコンテンツに使用された I PMP ツールの内容を I PMP 端末に通知することが、

5 データ暗号解読、透かしなどの I PMP ツールのカテゴリとして当該予め定めたテーブルから I PMP ツールタイプ ID を選択する手段と、

当該 I PMP ツールタイプ ID の下である特定のアルゴリズムを有するある特定の I PMP ツールに関して当該予め定めたテーブルから I PMP ツール ID を選択する手段と、

10 当該予め定めたテーブルから I PMP ツール位置 ID を選択して、I PMP ツールをダウンロード又は検索可能な場所を通知する手段と、

I PMP ツールを遠隔で検索する場合、当該 I PMP ツールリストに URL 位置を与える手段と、

15 バイナリフォーマットにプリコンパイルされた I PMP ツールの各セットに関する I PMP ツールフォーマット ID を選択する手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

11. 請求項 1、2、3 のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

20 イントラ符号化フレーム（I フレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索する手段と、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化する手段と、

25 を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

12. 請求項 1、2、3 のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索する手段と、  
すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重

要ビットのみを暗号化して、暗号解読側の処理を高速化する手段と、  
を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

5 13. 請求項 11 または 12 において選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行われた保護コンテンツストリームを復号する手段と、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読する手段と、

10 を含む、保護コンテンツを暗号解読して再生する I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

14. 指定インタフェースに従って I PMP ツールがされており、

当該インタフェースを含んだ I PMP 端末が構築された I PMP システムの装置において、

15 当該 I PMP ツールを検索して当該端末の当該インタフェースに適合させる手段

を含む、コンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

15. MPEG-4 システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定し、

20 MPEG-4 の I PMP 基本ストリームに I PMP ツールを保持することを可能にした、コンテンツ提供及び保護用の柔軟及び共通 I PMP システムの装置。

16. 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

25 データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

透かしツールを用いて当該コンテンツに透かし情報を埋め込むステップと、

上記ステップで用いられた当該コンテンツに関するコンテンツ ID 及び I PMP (知的所有権管理保護) ツールリスト (I PMP ツール情報) を作成するステ



ップと、

各コンテンツストリームのヘッダとして保持すべき I P M P ツールリストフラグを作成するステップと、

5 I P M P ツールリストフラグ、次いで I P M P ツールリスト、コンテンツ I D 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I P M P システムの方法。

10 17. 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツール又は他のツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

15 上記ステップで用いた当該コンテンツに関するコンテンツ I D 及び I P M P (知的所有権管理保護) ツールリスト (I P M P ツール情報) を作成するステップと、

各コンテンツストリームのヘッダとして保持すべき I P M P ツールリストフラグを作成するステップと、

20 I P M P ツールリストフラグ、次いで I P M P ツールリスト、コンテンツ I D 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I P M P システムの方法。

18. 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

25 暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化するステップと、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化するステップと、

当該コンテンツストリームと同一のストリームに保持された I P M P 情報に上

記当該暗号化されたキーを埋め込むステップと、

上記ステップで用いた当該コンテンツに関するコンテンツID及びIPMP（知的所有権管理保護）ツールリスト（IPMPツール情報）を作成するステップと、

- 5       各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成するステップと、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

- 10       を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟IPMPシステムの方法。

19.   請求項16、17、18のいずれかにおいて当該コンテンツに関するコンテンツID及びIPMPツールリストを作成することが、

- 15       IPMPツールIDを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示するステップと、

位置タイプIDを各IPMPツールに割当てて、当該IPMPツールが入手可能である位置のタイプを通知するステップと、

- 20       フォーマットIDを割当てて、ダウンロードされたIPMPツールフォーマットを表示して、準拠IPMP端末がそれらのプラットフォームに基づいて選択及び検索することを可能にするステップと、

当該IPMPツールの位置を表示して、端末が当該IPMPツールを当該位置から取得することを可能にするステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟IPMPシステムの方法。

- 25       20.   IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテ

ンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得するステップと、

を含む、 I PMP 端末側のコンテンツ提供及び保護用の柔軟 I PMP システムの方法。

- 5        21.     I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

        I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈するステップと、

- 10        ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得するステップと、

        要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

- 15        前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

        前記ユーザ権利認証が成功した後、要求されたコンテンツの消費の消費規則を取得するステップと、

        を含む、 I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

- 20        22.     要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

        前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

        当該ライセンス又はキー情報を I PMP 端末で構文解析するステップと、

- 25        当該ライセンス又はキー情報を当該 I PMP 端末のメモリに格納するステップと、

        当該 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

        I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解

釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該I PMPツールリストに基づいてI PMPツールを取得するステップと、

- 5       I PMPツールリスト情報の当該部分と共に上記ステップで検索された当該I PMPツールを当該I PMP端末のメモリに格納するステップと、

当該メモリに格納された当該I PMPツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号するステップと、  
を含む、I PMP端末側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの方法。

10

23.   要求をコンテンツディストリビュータに送信して、ユーザ認証を行うステップと、

当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

- 15       当該ライセンス又はキー情報をI PMP端末で構文解析するステップと、  
      当該ライセンス又はキー情報を当該I PMP端末のメモリに格納するステップと、

当該I PMP端末のI PMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

- 20       I PMPツールリストフラグ、コンテンツID及びI PMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該I PMPツールリストに基づいてI PMPツールを取得するステップと、

- 25       I PMPツールリスト情報の当該部分と共に上記ステップで検索された当該I PMPツールを当該I PMP端末のメモリに格納するステップと、

当該ライセンス又はキー情報を用いて当該I PMP情報内の当該暗号化されたキーを暗号解読するステップと、

コンテンツプロバイダ側で当該コンテンツを上記ステップで暗号化するために

使用された暗号化キーを取得するステップと、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得するステップと、

当該最初のコンテンツを当該 I PMP 端末で再生する為に復号するステップと、  
5   を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

24.   請求項 20、21、22、23 のいずれかにおいてローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得することが、

10   I PMP ツールの大部分に関する I PMP ツール ID をテーブルに定義されており、

今後の又は未知／専用の I PMP ツールに使用されるべき I PMP ツール ID に関する項目を当該テーブルに予約する余地があり、

15   I PMP ツールタイプとも呼ばれる I PMP ツールのカテゴリとして I PMP ツール ID の一部が定義されている、

当該テーブルを I PMP 端末に事前ロード、事前符号化又はダウンロードするステップと、

前記コンテンツストリーム内に保持された当該 I PMP ツールリストから当該 I PMP ツール ID を抽出するステップと、

20   前記コンテンツストリームに保持された当該 I PMP ツールリストに表示された I PMP ツール位置識別子を取得するステップと、

I PMP ツール位置識別子に加えて、I PMP ツール ID と共に、当該コンテンツストリームに保持された I PMP ツールフォーマット ID を取得するステップと、

25   適切なフォーマットである I PMP ツールを選択して、I PMP 端末プラットフォームに適合させるステップと、

上記手段で取得された当該位置から当該 I PMP ツールを検索するステップと、  
を更に含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

25. 予め定めたテーブルに基づいてI PMPツールリストを構築して、コンテンツに使用されたI PMPツールの内容をI PMP端末に通知するステップと、  
対応するコンテンツストリームの前に当該I PMPツールリストを挿入するステップと、

5 を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの方法。

26. 予め定めたテーブルに基づいてI PMPツールリストを構築してコンテンツに使用されたI PMPツールの内容をI PMP端末に通知することが、

データ暗号解読、透かしなどのI PMPツールのカテゴリとして当該予め定めた  
10 テーブルからI PMPツールタイプIDを選択するステップと、

当該I PMPツールタイプIDの下である特定のアルゴリズムを有するある特定のI PMPツールに関して当該予め定めたテーブルからI PMPツールIDを選択するステップと、

当該予め定めたテーブルからI PMPツール位置IDを選択して、I PMPツールをダウンロード又は検索可能な場所を通知するステップと、  
15

I PMPツールを遠隔で検索する場合、当該I PMPツールリストにURL位置を与えるステップと、

バイナリフォーマットにプリコンパイルされたI PMPツールの各セットに関するI PMPツールフォーマットIDを選択するステップと、

20 を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの方法。

27. 請求項16、17、18のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

イントラ符号化フレーム（Iフレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索するステップと、  
25

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化するステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共

通 I PMP システムの方法。

28. 請求項 16、17、18 のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索するステップと、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重要ビットのみを暗号化して、暗号解読側の処理を高速化するステップと、  
を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

29. 請求項 27 または 28 において選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行うことが、

保護コンテンツストリームを復号するステップと、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読するステップと、

を含む、保護コンテンツを暗号解読して再生する I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

30. MPEG-4 システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定して、

MPEG-4 の I PMP 基本ストリームに I PMP ツールを保持することを可能にした、コンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

31. 暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つプロバイダと、ネットワークを通じて接続されたユーザ端末から構成され、プロバイダ側で、ユーザ端末に送るメッセージ中に、更新すべきソフトウェアモジュールの識別子とその存在する場所を示す情報を含めることにより、ユーザ端末に著作権保護システムの更新を行わせ、更新すべきソフトウェアモジュールは、解読モジュールと利用規則管理モジュールを含むことにより、プロバイダの意図する利用規則に従ってコンテンツの解読・視聴を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び変

通 I PMP システムの装置。

3 2. 暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つプロバイダと、ネットワークを通じて接続されたユーザ端末から構成され、ユーザ端末は、プロバイダから利用規則管理モジュールを受け取って自身に組み込み、これを用いて、プロバイダから受け取る著作権保護情報の中にある、コンテンツの利用規則に従い、プロバイダから受け取るコンテンツの再生を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

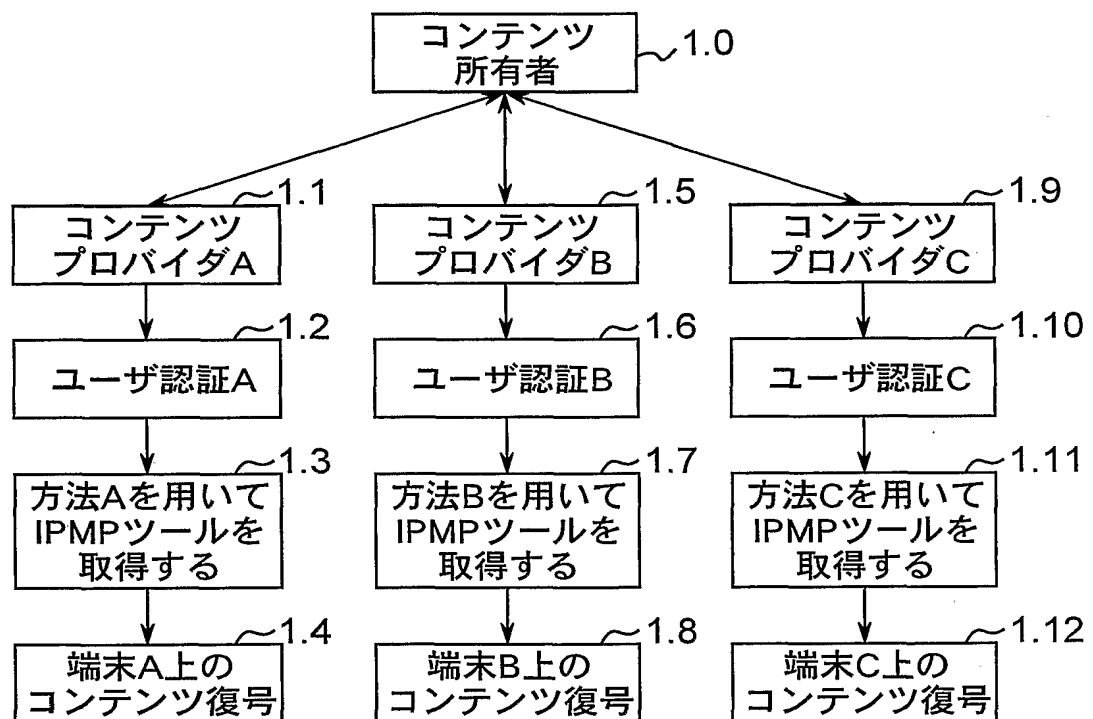
3 3. 利用規則は、コンテンツの利用可能期間、無料再生可能時間、再生可能回数、コピー可能回数、移動可能回数のいずれかを含むことを特徴とする請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

3 4. プロバイダからユーザ端末に送られるメッセージは、メッセージ項目名と直後に続くメッセージ項目の値の組で構成され、ユーザ端末に送るメッセージ項目の順序を問わないことを特徴とする、請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

3 5. ユーザ端末からプロバイダに送られるメッセージは、ユーザ端末情報を含むことにより、ユーザ端末に適合するモジュールをプロバイダから受信することが出来ることを特徴とする請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。



Fig. 1



2/12

Fig. 2

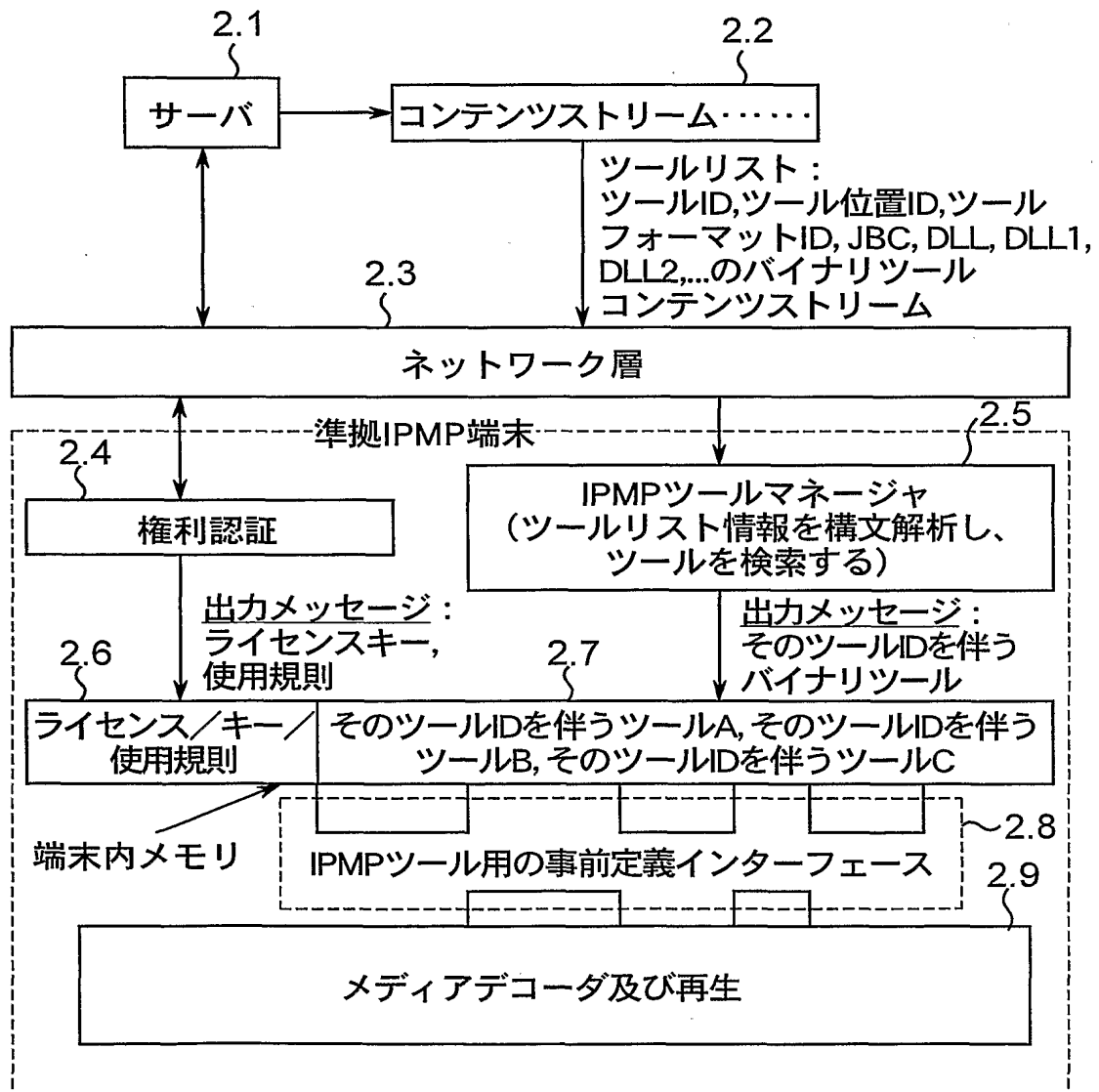
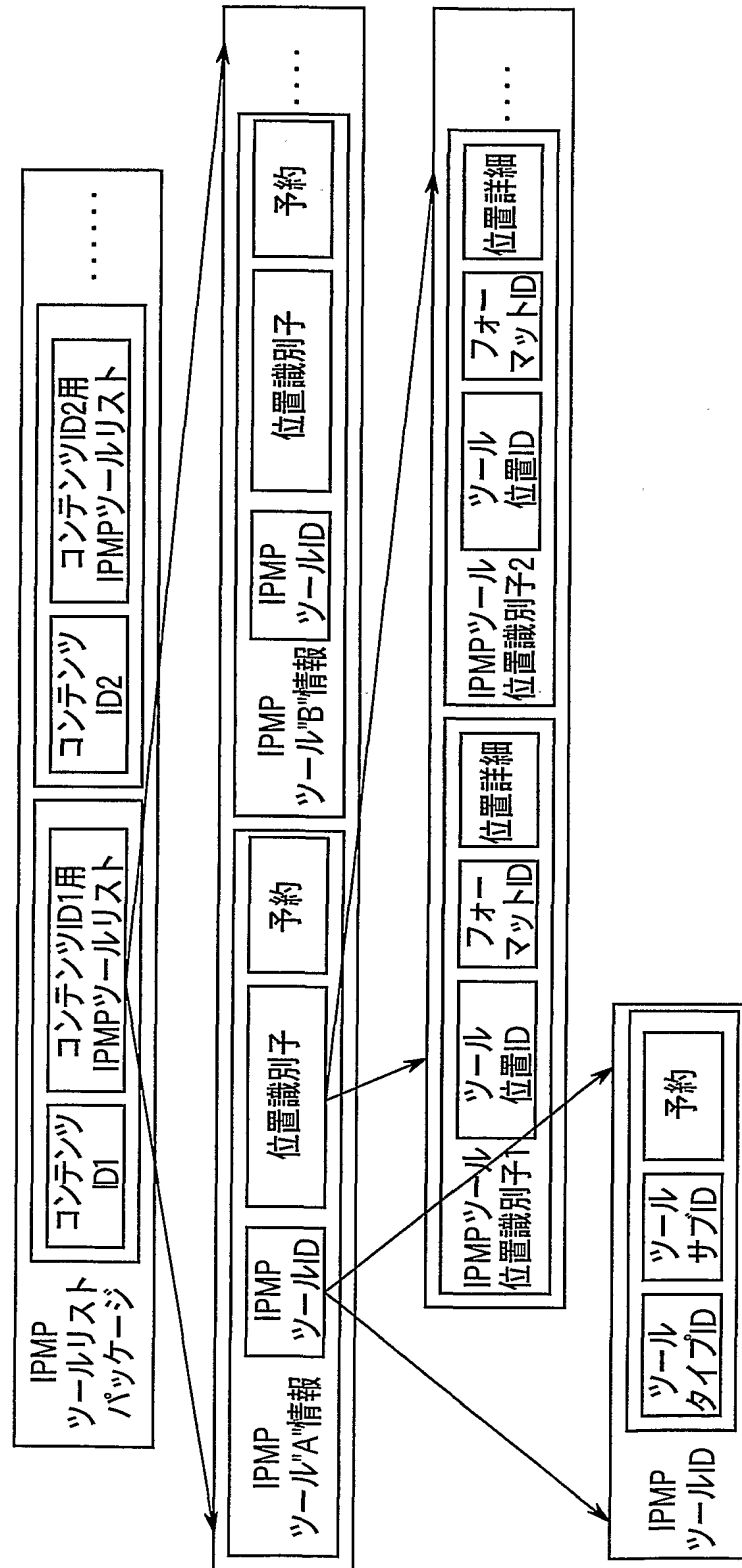


Fig.3



4/12

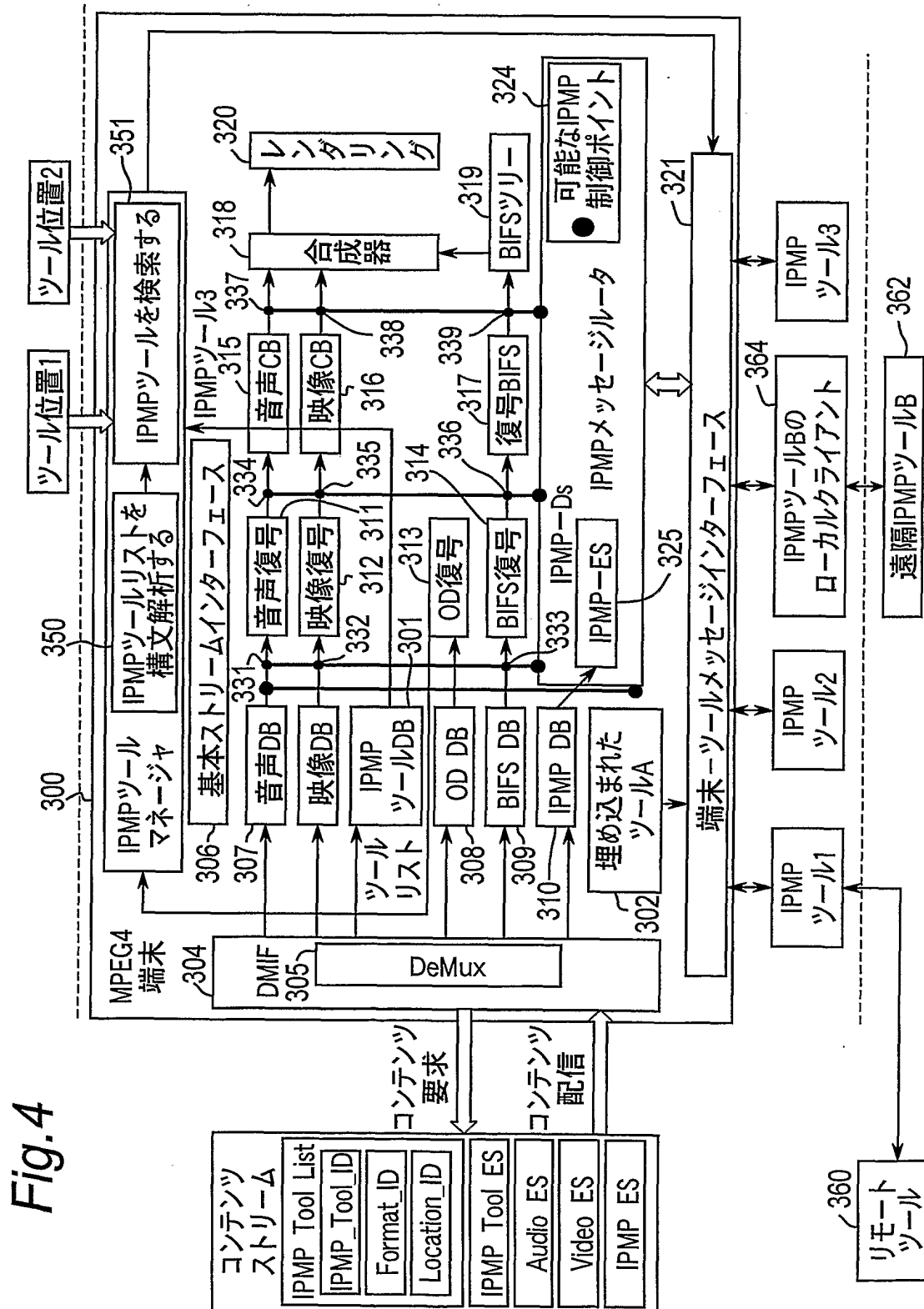
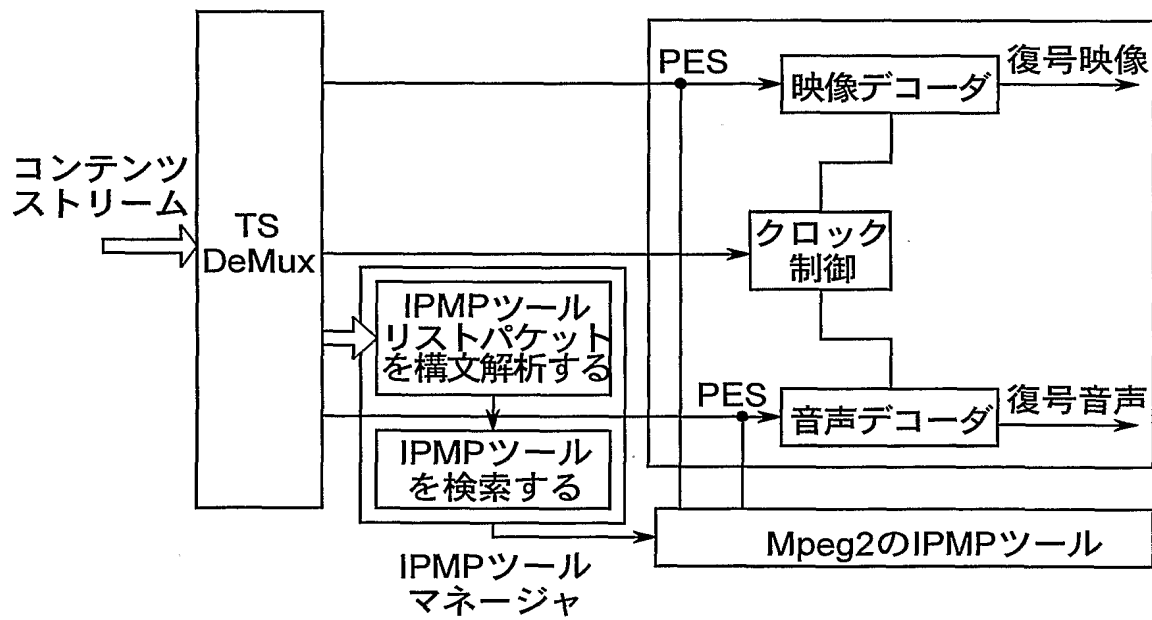
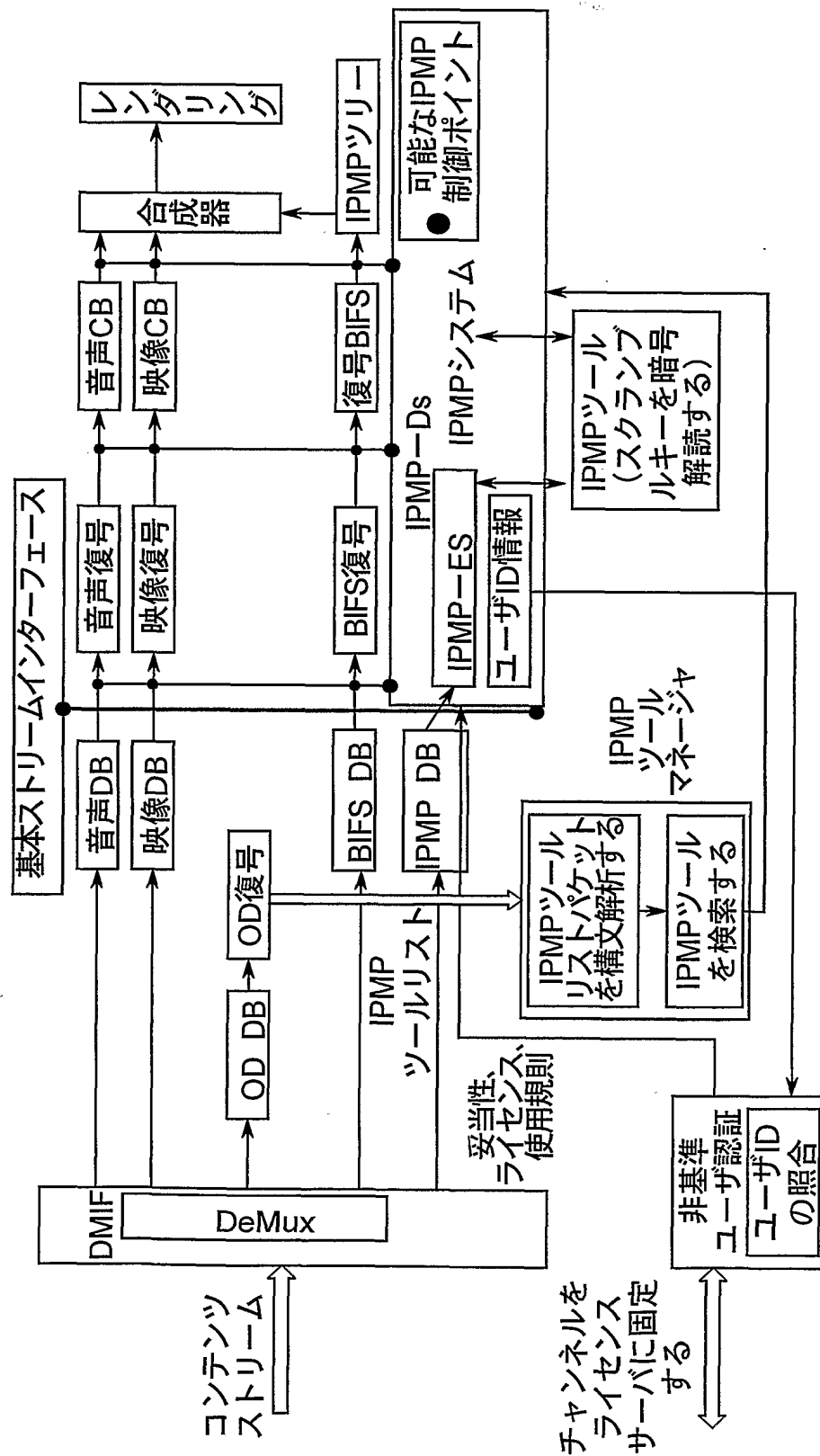


Fig.5



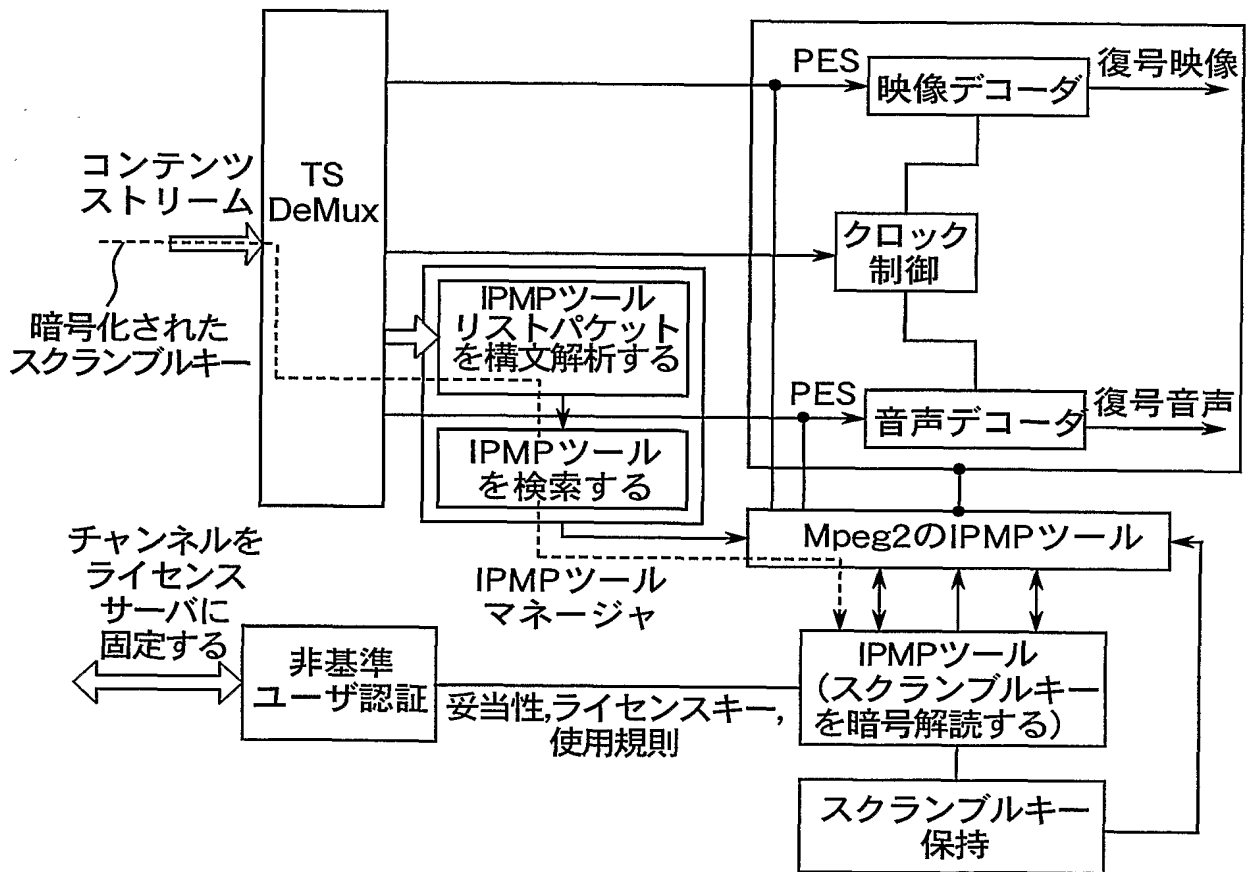
6/12

Fig.6



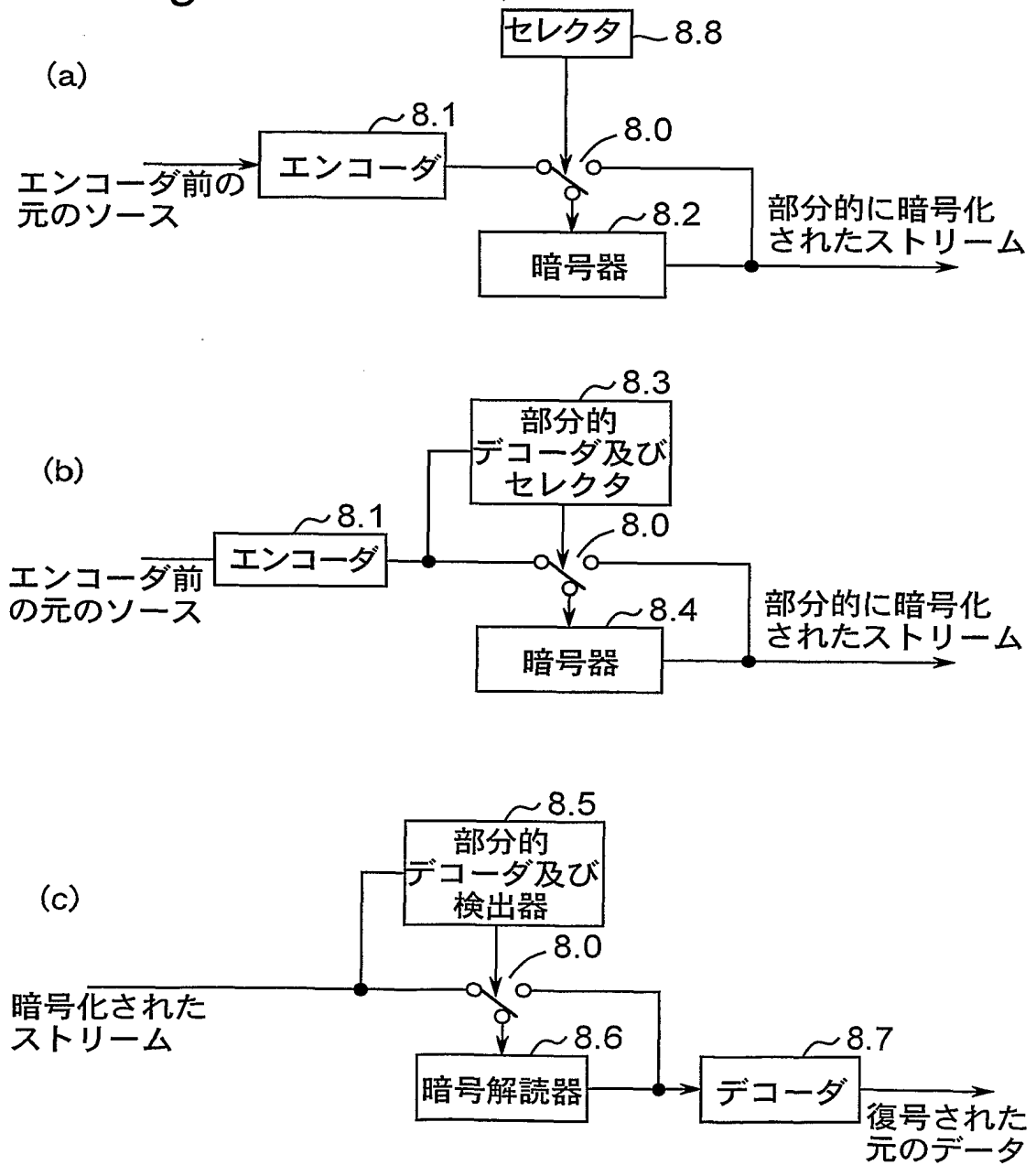
7/12

Fig. 7



8/12

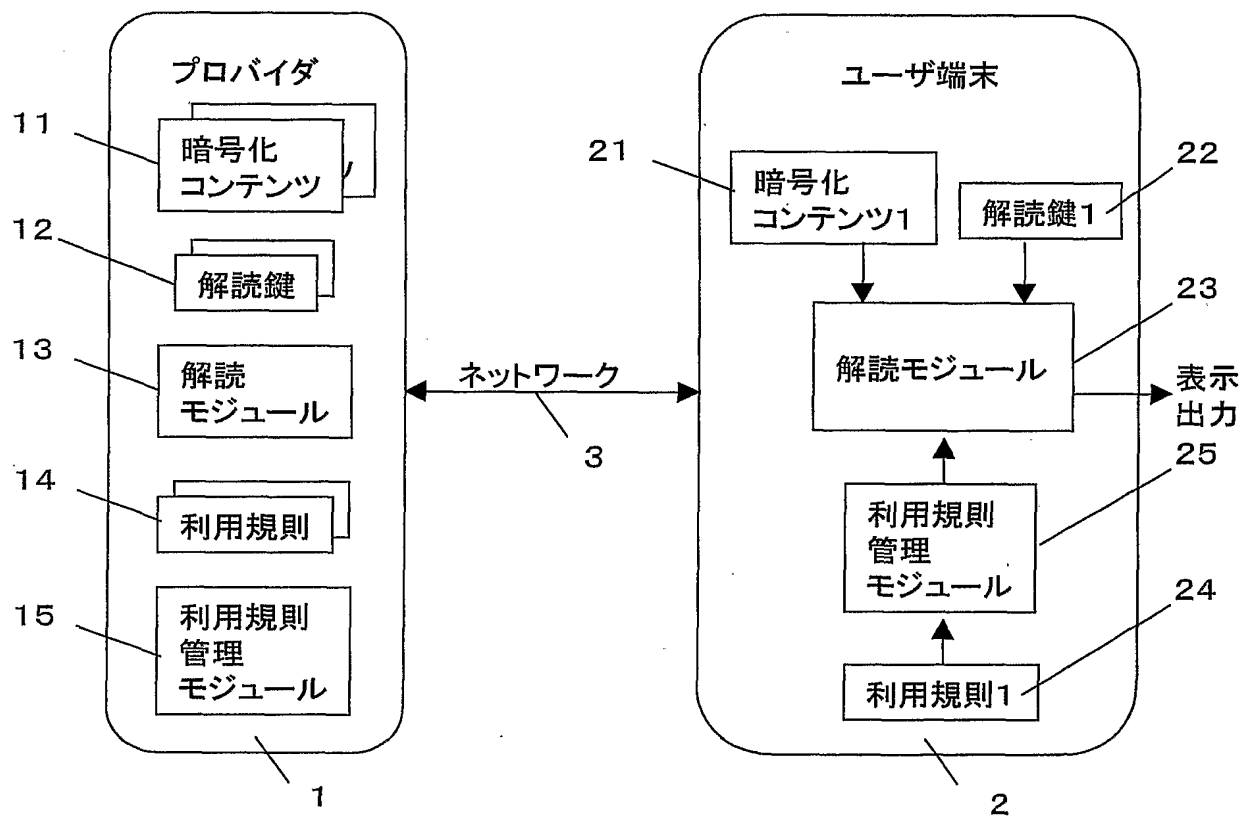
Fig. 8





9/12

Fig. 9



10/12

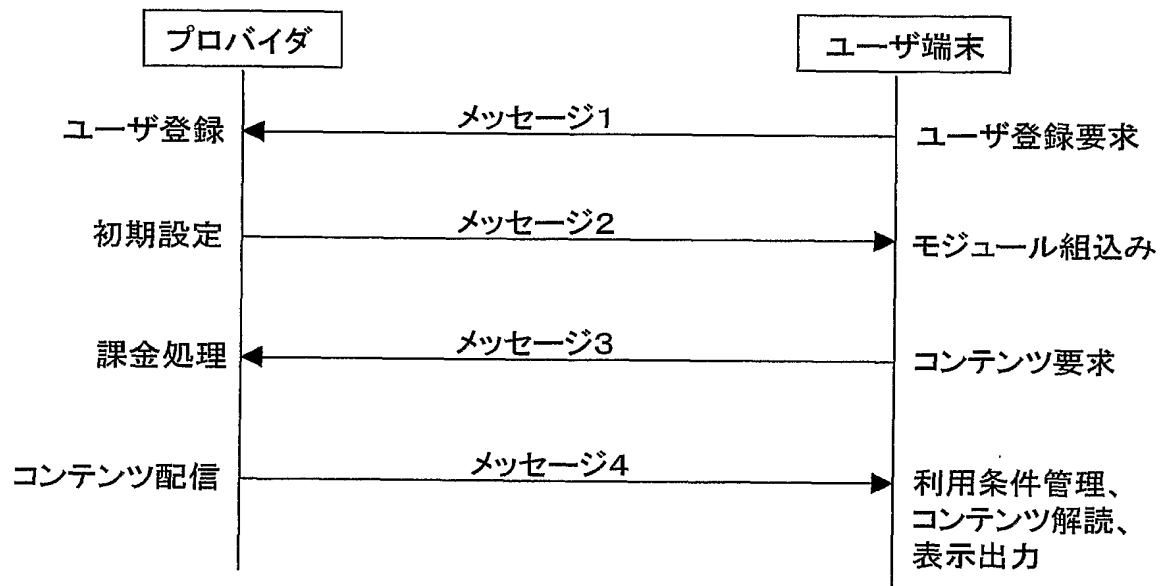
*Fig. 10*

Fig. 11

11/12

## メッセージ1

|          |            |
|----------|------------|
| メッセージID＝ | ユーザ登録      |
| ユーザ名＝    | 松下 太郎      |
| 支払い方法＝   | クレジットカード番号 |
| ユーザ端末情報＝ | Windows OS |

## メッセージ2

|            |                       |
|------------|-----------------------|
| メッセージID＝   | 初期設定                  |
| ユーザID＝     | XYZ                   |
| IPMP情報＝    | コンテンツリスト              |
| IPMPツール情報＝ | 解読モジュールID, ロケーション     |
| IPMPツール情報＝ | 利用規則管理モジュールID, ロケーション |

## メッセージ3

|          |          |
|----------|----------|
| メッセージID＝ | コンテンツ要求  |
| ユーザID＝   | XYZ      |
| コンテンツ情報＝ | コンテンツ1ID |

## メッセージ4

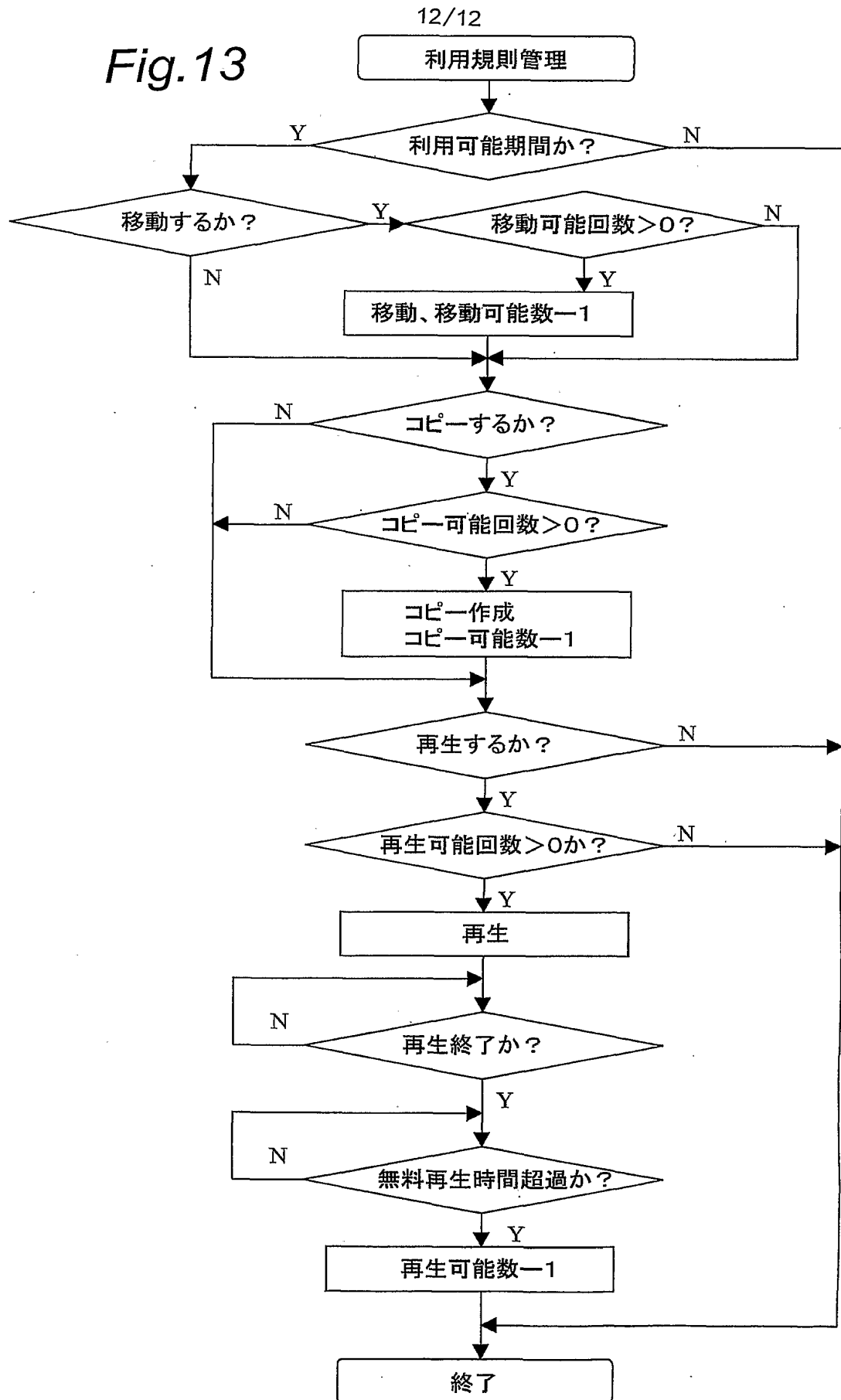
|          |           |
|----------|-----------|
| メッセージID＝ | コンテンツ配信   |
| IPMP情報＝  | 利用規則1     |
| IPMP情報＝  | 解読鍵1      |
| コンテンツ情報＝ | 暗号化コンテンツ1 |

Fig. 12

## 利用規則1

|          |                    |
|----------|--------------------|
| 利用可能期間＝  | 2001.6.1-2001.6.30 |
| 無料再生時間＝  | 1分                 |
| 再生可能回数＝  | 3                  |
| コピー可能回数＝ | 1                  |
| 移動可能回数＝  | 5                  |

Fig.13



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05468

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L9/14, G06F17/60, G10L19/00, H04N7/08, H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L9/14, G06F17/60, G10L19/00, H04N7/08, H04N7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

|                           |           |                            |           |
|---------------------------|-----------|----------------------------|-----------|
| Jitsuyo Shinan Koho       | 1922-1996 | Toroku Jitsuyo Shinan Koho | 1994-2002 |
| Kokai Jitsuyo Shinan Koho | 1971-2002 | Jitsuyo Shinan Toroku Koho | 1996-2002 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE(JOIS), WPI, INSPEC(DIALOG), IPMP

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|-----------|---|-----------------------|
| Y         | OPIMA Specification Version 1.1. [online],<br>27 June, 2000 (27.06.00),<br>[retrieved on 2002-08-30]. Retrieved from the<br>Internet:<URL:http://leonardo.telecomitalialab.co<br>m/opima/>, especially 2.4 Protocols,<br>3.3.3.2 getImpSystem | 1-13,16-29,<br>31-35  |
| Y         | WO 99/48296A (INTERTRUST TECHNOLOGIES CORPORATION),<br>23 September, 1999 (23.09.99),<br>Page 25, line 25 to page 26, line 14<br>& EP 1062812 A & CN 1301459 A<br>& JP 2002-507868 A  | 1-13,16-29,<br>31-35  |
| A         | MPEG-4 Intellectual Property Management &<br>Protection(IPMP) Overview & Applications. [online],<br>1998.12, [retrieved on 2002-08-30]. Retrieved<br>from the Internet: <URL:http:<br>//mpeg.telecomitalialab.com/working_documents.htm<br>>  | 1-13,16-29,<br>31-35  |

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

|   |  |
|---|--|
| * Special categories of cited documents:  | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |
| "A" document defining the general state of the art which is not considered to be of particular relevance  | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |
| "E" earlier document but published on or after the international filing date  | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |  |

Date of the actual completion of the international search  
12 September, 2002 (12.09.02)Date of mailing of the international search report  
01 October, 2002 (01.10.02)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.  
Patent provided by Sughrue Mion PLLC - <http://www.sughrue.com>

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05468

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| A         | Intellectual Property Management and Protection in MPEG Standards. [online], 2001.01, [retrieved on 2002-08-30]. Retrieved from the Internet:<URL:http://mpeg.telecomitalia.com/standards/ipmp/>                 | 1-13,16-29,<br>31-35  |
| A         | Tadashi KANEKO, "MPEG-4 Chosakuken Kanri · Shien Field no Tokucho", Information Processing Society of Japan Kenkyu Hokoku, 30 January, 1999 (30.01.99), Vol.99, No.11, pages 25 to 32                            | 1-13,16-29,<br>31-35  |
| A         | Tadashi KANEKO, Ikuo KUDO, "MPEG-4 ni okeru Chosakuken Shikibetsu Kanri no Hyojun Doko ni tsuite", Information Processing Society of Japan Kenkyu Hokoku, 29 May, 1998 (29.05.98), Vol.98, No.52, pages 75 to 82 | 1-13,16-29,<br>31-35  |

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05468

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 14, 15, 30

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The claims 14, 15, and 30 are so unclear that no meaningful international search can be carried out.

3. ☐ Claims Nos.:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-4, 11-13, 16-19, 27-29
2. Claims 5-9, 20-24
3. Claims 10, 26
4. Claim 25
5. Claims 31-35

Claims 14, 15, and 30 fall in the Japanese Law Concerning International Applications, Etc. Pursuant to PCT, Article 8, Paragraph 2, Subparagraph 2 (PCT Article 17(2)) and no meaningful international search can be carried out. Accordingly, these claims are not included in any of the aforementioned groups of inventions.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

|  |   |                       |
|--|---|-----------------------|
| A. 発明の属する分野の分類 (国際特許分類 (IPC))  |   |                       |
| Int. Cl <sup>7</sup> H04L9/14 G06F17/60 G10L19/00 H04N7/08 H04N7/167   |   |                       |
| B. 調査を行った分野  |   |                       |
| 調査を行った最小限資料 (国際特許分類 (IPC))   |   |                       |
| Int. Cl <sup>7</sup> H04L9/14 G06F17/60 G10L19/00 H04N7/08 H04N7/167   |   |                       |
| 最小限資料以外の資料で調査を行った分野に含まれるもの   |   |                       |
| 日本国実用新案公報 1922-1996年<br>日本国公開実用新案公報 1971-2002年<br>日本国登録実用新案公報 1994-2002年<br>日本国実用新案登録公報 1996-2002年   |   |                       |
| 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)  |   |                       |
| JICSTファイル (JOIS), WPI, INSPEC (DIALOG)<br>IPMP   |   |                       |
| C. 関連すると認められる文献  |   |                       |
| 引用文献の<br>カテゴリー*  | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号      |
| Y  | OPIMA Specification Version 1.1. [online], 2000.06.27,<br>[retrieved on 2002-08-30]. Retrieved from the Internet:<br><URL:http://leonardo.telecomitalialab.com/opima/>,<br>especially 2.4 Protocols, 3.3.3.2 getImpSystem | 1-13, 16-29,<br>31-35 |
| Y  | WO 99/48296 A (INTERTRUST TECHNOLOGIES CORPORATION)<br>1999.09.23, 第25頁第25行-第26頁第14行 & EP 1062812 A &<br>CN 1301459 A & JP 2002-507868 A  | 1-13, 16-29,<br>31-35 |
| <input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。  |   |                       |
| * 引用文献のカテゴリー<br>「A」 特に関連のある文献ではなく、一般的技術水準を示すもの<br>「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの<br>「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)<br>「O」 口頭による開示、使用、展示等に言及する文献<br>「P」 国際出願日前で、かつ優先権の主張の基礎となる出願        |   |                       |
| の日の後に公表された文献<br>「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの<br>「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの<br>「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの<br>「&」 同一パテントファミリー文献 |   |                       |
| 国際調査を完了した日   | 国際調査報告の発送日  |                       |
| 12.09.02   | 01.10.02  |                       |
| 国際調査機関の名称及びあて先<br>日本国特許庁 (ISA/JP)<br>郵便番号100-8915<br>東京都千代田区霞が関三丁目4番3号   | 特許庁審査官 (権限のある職員)<br>中里 裕正   | 5M 9364               |
|  | 電話番号 03-3581-1101   | 内線 3597               |



| C (続き) . 関連すると認められる文献 |   |                       |
|-----------------------|---|-----------------------|
| 引用文献の<br>カテゴリー*       | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示   | 関連する<br>請求の範囲の番号      |
| A                     | MPEG-4 Intellectual Property Management & Protection(IPMP)<br>Overview & Applications. [online], 1998.12,<br>[retrieved on 2002-08-30]. Retrieved from the Internet:<br><URL:http://mpeg.telecomitalia.com/working_documents.htm> | 1-13, 16-29,<br>31-35 |
| A                     | Intellectual Property Management and Protection in<br>MPEG Standards. [online], 2001.01,<br>[retrieved on 2002-08-30]. Retrieved from the Internet:<br><URL:http://mpeg.telecomitalia.com/standards/ipmp/>                        | 1-13, 16-29,<br>31-35 |
| A                     | 金子格,<br>MPEG-4 著作権管理・支援フィールドの特徴,<br>情報処理学会研究報告, 1999.01.30, Vol.99, No.11, p.25-32  | 1-13, 16-29,<br>31-35 |
| A                     | 金子格, 工藤育男,<br>MPEG-4 における著作権識別管理の標準動向について,<br>情報処理学会研究報告, 1998.05.29, Vol.98, No.52, p.75-82  | 1-13, 16-29,<br>31-35 |

## 第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☒ 請求の範囲 14, 15, 30 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、  
請求の範囲の記載が著しく不明確であるため、有効な国際調査をすることができない。
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

1. 請求の範囲 1-4, 11-13, 16-19, 27-29
2. 請求の範囲 5-9, 20-24
3. 請求の範囲 10, 26
4. 請求の範囲 25
5. 請求の範囲 31-35

請求の範囲 14, 15, 30 は、法第8条第2項第2号に該当し (PCT 17条(2))、国際調査を行うことができないので、どの発明にも含まれていない。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。